Tab B

Preliminary Research and Development Roadmap for Protecting and Assuring the Energy Infrastructure*

* This document is one component of a longer report entitled *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures* (Transition Office of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office. Washington, D.C. July 1998). For more information, please see <URL:http://www.ciao.gov/>.

Contents

Section 1 Introduction B-1

1.1 Scope of the Infrastructure B-1
1.1.1 Electric Power B-1
1.1.2 Oil and Natural Gas B-2
1.2 Characterization of the Infrastructure B-3
1.2.1 Electric Power B-3
1.2.2 Oil and Natural Gas B-5
1.3 Issues and Trends B-6
1.3.1 Electric Power B-6
1.3.2 Oil and Natural Gas B-8
1.3.3 Challenges in the Energy Industry B-8
1.3.4 Ultimate Energy Industry Configurations B-9

Section 2 Threats and Vulnerabilities B-11

2.1 Threats B-11
2.2 Vulnerabilities B-13
2.2.1 Electric Power B-13
2.2.2 Oil and Gas B-14

Section 3 R&D Topics and Activities B-17

3.1 Electric Power Systems B-18
3.1.1 Real-time Control Mechanisms B-18
3.1.2 Analysis of Scale and Complexity B-24
3.1.3 Vulnerability Assessment B-28
3.1.4 Information Assurance and Cyber Security B-31
3.1.5 Emergency Response and Recovery Information Technologies B-39
3.1.6 Transmission and Distribution Technologies B-43
3.1.7 On-line Security Assessment B-48
3.1.8 Dispersed Generation and Backup Infrastructures B-51
3.2 Oil and Natural Gas Systems B-54
3.2.1 Critical Consequence Analysis B-54
3.2.2 Decision Support Systems B-56
3.2.3 Physical Protection Assessment B-63
3.2.4 Multisensor and Warning Technologies B-65
3.2.5 Emergency Response Capability Enhancement B-68
3.2.6 Cyber Protection Enhancement B-70

Contents (Cont.)

3.3 Joint Topics B-74
3.3.1 Evaluation of Policy Effects B-74
3.3.2 Institutional Barriers B-77
3.3.3 Infrastructure Interdependencies B-80
3.4 Summary of Research Topics B-83

Section 4 R&D Topic Roadmap B-91

Tables

B.1 Estimated Timeframe for Developing Real-time Control Technologies B-25

B.2 Estimates of Timeframe and Cost for Information Assurance and Cyber Security B-39

B.3 Assessment of the Complexity of Decision Analysis Models by Industry Sector B-61

B.4 Summary of Research Topics B-84

B.5 Summary of Funding Requirements by Research Topic B-90

B.6 Summary of the Energy R&D Roadmap B-92

Figures

B.1 U.S. Bulk Electric Power System Interconnections and Reliability Coordinators B-4

B.2 Spectrum of National Security Preparedness and Government Roles for the Electric Power System Infrastructure B-40

Section 1
Introduction

The security, economic prosperity, and social well being of the United States depend on a complex system of interdependent infrastructures. Their lifeblood is energy, an infrastructure composed of industries that produce and distribute electric power, oil, and natural gas.[1] Individuals and organizations in the United States spend approximately $500 billion per year, or about 7.5% of the gross national product, on electricity and fuels. Because specific complexities and characteristics of the electric power system (EPS) infrastructure differ from those of the oil and gas transportation and storage infrastructure, they are often described separately in this report.

1.1 Scope of the Infrastructure

1.1.1 Electric Power

The EPS infrastructure includes generation stations, transmission and distribution networks, and transport and storage of fuel needed to make and supply reliable electricity to customers at a reasonable cost. Electric utilities estimate that revenue from retail sales of electricity totaled $208 billion in 1995. More than one-third of the nation's primary sources of energy (i.e., coal, oil, gas, nuclear) is consumed to generate electricity.

Without electric power, other critical infrastructures, such as telecommunications, banking and finance, and segments of the transportation industry, could not function at an acceptable level. For example, power outages affect virtually all modes of transportation, including subways, elevators, and street traffic (e.g., traffic lights, gasoline pumps). Some infrastructures have invested in backup generating equipment to minimize the impact of a serious outage.

Consumers expect electricity to be available instantly — at the "flick of a switch." Major outages, such as those in the western United States on July 2 and August 10, 1996 (which affected 7.5 million customers), led to follow-up investigations to pinpoint causes

[1] Coal-related issues were not addressed directly, but Tab D, which discusses the transportation infrastructure, covers many issues related to coal delivery.

and suggest responses to reduce the possibility of future outages. President Clinton noted in his July 3, 1996, memo to the Secretary of Energy that the July 2 outage:

> … had a ripple effect as power stations across the vast grid automatically shut down as the result of experiencing a surge. The outages caused numerous problems in the region, including disruptions of train service, traffic problems, loss of air conditioning, interruption of telephone service, and interference with water supplies. … A steady supply of power is a vital factor in both the local and national economies and is essential for the safety of all Americans.

An electrical outage can result in both direct impacts (e.g., malfunctioning alarm systems) and indirect impacts (e.g., traffic accidents, looting). Analyses have shown that electrical power outages incur substantial costs. The 1977 New York City outage affected about 3 million customers and cost nearly $800 million (1995 dollars). Cost estimates from the August 1996 outage in the western United States have ranged from $700 million to $4 billion.

1.1.2 Oil and Natural Gas

Industry and consumers use petroleum as fuel and as lubrication for many modes of transportation (e.g., automobiles, commercial vehicles, agricultural equipment, trains, ships, aircraft) and industrial machinery. Petroleum products provide heat for residential, industrial, and commercial buildings and for producing, processing, packaging, distributing, and preparing food and food products. Petroleum also is used in the textile and clothing industries to manufacture synthetic fabric, detergents, and dry-cleaning solvents. Other uses for petroleum are with chemicals for cosmetics and pharmaceutical products, and with plastics in manufactured products. Petroleum also helped to generate 3% of electricity in the United States during 1996.

Natural gas is delivered to millions of consumers through the nation's 1.3-million-mile network of underground pipe (e.g., gathering, transmission, distribution). In 1995, the industry served 58.7 million customers: 53.9 million residential customers, 4.5 million commercial customers, 180,900 industrial end users, and 61,300 other customers. Electric power generators increasingly use natural gas. Also, gas technologies are increasing the market share in cooling applications and in gas-fueled vehicles. Furthermore, natural gas is the primary fuel used in cogeneration, capturing about 60% of the market. It is the cleanest burning fossil fuel, producing primarily carbon dioxide (CO_2), water vapor, and small amounts of nitrogen oxides.

The oil and gas industries are vital to the U.S. economy because they provide:

- Energy to more than 260 million Americans,
- 65% of the nation's energy needs,

- 1.5 million jobs, and
- Annual revenues of almost $400 billion.

The shock of rapid increases in the price of oil in the 1970s demonstrated that large, sudden price increases erode purchasing power and may drive the global economy into recession. Between 1972 and 1991, price shocks alone cost the U.S. economy $4 trillion. Underneath the economic issues lie hard facts. Most Americans could not heat their homes, cook their food, or drive their vehicles without oil and gas. These infrastructure commodities are the foundation of modern society, and the United States is highly dependent on them.

Despite this dependence, the U.S. energy infrastructure is among the most reliable and robust in the world. While widespread energy shortages and outages make national and international news, they are rare. Most incidents occur at the local level and do not propagate. Despite the reliability of the U.S. energy infrastructure, however, challenges exist for sustaining this resilience as our nation enters the millenium. The oil and gas infrastructures represent a large capital investment and have become increasingly vulnerable to outside forces.

1.2 Characterization of the Infrastructure

1.2.1 Electric Power

The U.S. electric power system is complex. Generating units produce electricity; transmission lines transport large quantities of electricity long distances over high-voltage lines; and distribution lines deliver small amounts of electricity to individual customers over low-voltage lines. Substations, or places where power transformers increase voltage to transmit electricity or decrease voltage to distribute power, link the system. Energy or utility control centers coordinate operations.

The EPS includes approximately 3,200 electric utilities throughout the 50 states, the District of Columbia, and Mexico and is closely tied to Canadian power systems. Traditional electric utilities generate, transmit, and distribute electricity and other energy services in designated service territories. Restructuring has encouraged new entities, such as nonutility power producers, power marketers, and power brokers, to enter the emerging market.

At the end of 1994, U.S. electric utilities owned 10,427 generating units. The total installed capacity in 1995 exceeded 769,000 MW, and net generation totaled 3,356 billion kilowatt-hours. Total generation increased by approximately 3% in 1995.

Coal generating units continue to provide the largest share of electric energy (55%) and have the largest share of generating capacity (43%). Nuclear power accounts for 22% of generation and 14% of capacity. Oil and gas units provide 12% of energy but

have a 29% share of capacity because these sources are used more for peaking and daily cycling. Renewables (primarily hydroelectric) represent about 10% of generation and 11% of capacity. The remaining capacity (3%) is hydroelectric pumped storage.

Electric utilities use the ultimate "just-in-time" delivery system. Consumers challenge the system by using lights, appliances, motors, and other electrical equipment. In the aggregate, the instantaneous turning on and off of lights, appliances, computers, and other equipment connected to the EPS requires rapid response by the combined generation, transmission, and distribution portions of the system to maintain frequency, voltage, and dynamic stability. With more and more devices being produced to operate using electricity, more remote controls and more reliance on computers, the U.S. has become increasingly dependent on electricity. The continuity of high-quality electricity is more critical than ever to ensure electric power to our electronically dependent society.

As shown in Figure B.1, bulk EPSs in the United States and Canada are structured into four major networks: Eastern, Western, ERCOT, and Quebec Interconnections.

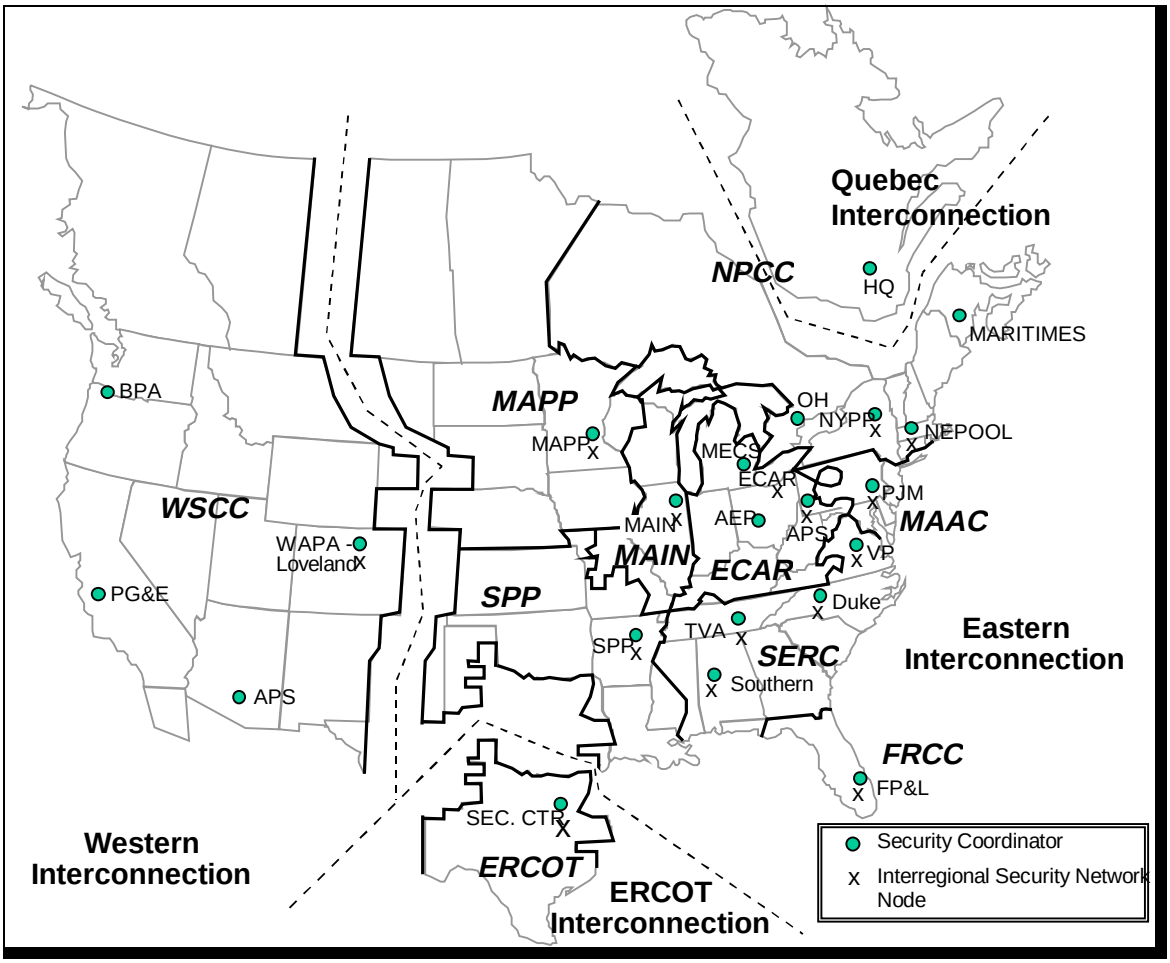

Figure B.1 U.S. Bulk Electric Power System Interconnections and Reliability Coordinators

Each interconnection consists of extra-high voltage connections between individual utilities, which transfer electricity from one part of the network to another. These interconnections are monitored and controlled to ensure safety and dependability. Each interconnection must balance supply and demand. Even the power exchanger between these interconnections must be carefully regulated in real time.

The North American Electric Reliability Council (NERC) is composed of 10 regional reliability councils shown in Figure B.1 (e.g., MAPP is the regional reliability council that covers five north central U.S. states and two Canadian provinces). Within each council are security coordinators, interregional security network nodes, and 146 control areas.

The EPS relies on a centralized control center (command-and-control infrastructure) to coordinate the overall operation of the system within control areas. A key component for communication between the control center and important equipment is the Supervisory Control and Data Acquisition (SCADA) system. Its primary purpose is to control generation and the transmission network directly within the area to balance power flows, regulate voltage, and control frequency. Imbalances between loads and generation are managed through real-time control of selected generators and, during severe emergencies, by controlled load shedding. System control in a restructured industry may change some of these responsibilities.

1.2.2 Oil and Natural Gas

The oil and natural gas industries are complex, robust networks that have proved to be extremely reliable over time. The industries can be characterized by production, transportation, processing, distribution, and end-use activities. Production involves well-heads that feed into gathering pipelines. These pipelines carry the crude oil or gas to processing centers: crude oil to a refinery and natural gas to a gas processing plant. Transmission pipelines deliver the gas or refined petroleum products to distribution pipelines that provide products to customers that range from bulk terminal operators to end users.

The delivery systems for natural gas and petroleum products include (in varying levels) compressor stations for natural gas and pumping stations for liquid products, storage capability, and market hubs. Both gas and oil systems use physically manipulated and automated controls, including SCADA. The natural gas system has city gates — transfer and transaction points for gas from the pipeline company to the local distribution company. Barges, trucks, and railroads also transport liquid products. End users include residential, commercial, and industrial customers, as well as electric utilities.

The gas and oil infrastructure is vast and reaches into every region of the country. About 22 trillion cubic feet of gas and 6.6 billion barrels of refined oil products are

delivered annually in the United States. In 1996, the oil and gas infrastructure included the following capabilities:

- Operation of 161 domestic refineries with crude distillation capacity of more than 15 million barrels per day. Refineries represent an infrastructure in their own right; the typical refinery is a collection of many manufacturing plants and supporting facilities, which operate interdependently. They convert crude oils and other raw materials into petroleum products.

- Crude oil and petroleum products pumped through about 220,000 miles of pipelines.

- Natural gas collected, transported, stored, and delivered through approximately 62,000 miles of gathering pipelines; 265,000 miles of transmission pipelines; and 935,000 miles of distribution pipelines.

- 375 natural gas storage fields.

1.3 Issues and Trends

1.3.1 Electric Power

When the EPS fails to meet our expectations, it can lead to significant personal or economic losses. Since the nation has entered the "communication age" and our society is increasingly dominated by "silicon-based" technologies, the requirements for electricity have changed. Our society previously needed large amounts of electricity to support our economy (primarily quantities of electrical supply). Now we not only require large amounts of electricity, but also a more reliable supply (both quantity and quality of supply are critical). Thus, the requirement for electric power assurance has increased and is likely to continue to increase. Reliability is a concern, and future reliability could be impaired by the increasing complexity of the grid, by various side effects due to restructuring, and by deliberate attacks.

Factors that could affect the traditional reliability and security of the EPS infrastructure include the following:

- Business elements, including new information systems for electronic commerce, data interchange, and improved operational efficiencies, are essential because of the rapid restructuring of the electric power and natural gas industries.

- Electric utility and natural gas companies are consolidating resources, but finding it nearly impossible to obtain new transmission line rights-of-way because of a prevailing "not-in-my-backyard" (NIMBY) attitude.[2]

[2] If everyone applies NIMBY, the result is BANANA (build absolutely nothing anywhere near anyone).

- With the advent of natural gas and electricity commodity markets, marketing companies have increased from 8 in 1992 to more than 250 in 1996. This increase has caused an exponential growth in the number and magnitude of power transactions and the resulting demands on the physical grid and its control system and on the information system needed to manage the transactions.

- Additional vulnerabilities have created a dependence on industry-wide information systems based on open-system architectures, centralized operations, increased communications over public switched networks, and remote maintenance.

- Downsizing in the industry has increased the probability of disgruntled "insiders" and has created a loss of expertise.

- A possible reduction in maintenance after restructuring could result in Auckland-type failures (e.g., cascading, or progressive, failure of a system).

- Because change has occurred so rapidly in the electric industry, vulnerabilities have been introduced (e.g., those related to restructuring and rapid proliferation of industry-wide information systems based on open-system architectures).

- Regulatory requirements for restructuring the industry have increased the size of the community that needs to be able to access industry data, while at the same time system control operations have been concentrated into fewer locations. Increased connectivity and a smaller number of increasingly critical sites create more opportunities for malicious acts.

Electronic power components also are changing the nature of the demand for electricity in less obvious ways, such as adjustable speed drives, which can destroy the overall integrity of the system. While these drives generally are desirable from the user's viewpoint because they eliminate problems associated with slight variations in the voltage or frequency of the grid, they also remove the "natural" tendency of loads to reduce their value as either the voltage or the frequency is reduced. Generally, a system under near-failure conditions reduces voltage and frequency. However, adjustable speed drives do not perform in this way unless they are programmed to do so. Adjustable speed drives not only compromise system integrity, but they also are applied when simpler solutions are available. Finally, top-changing transformers automatically switch secondary winding tops to sustain voltage or feeders.

1.3.2 Oil and Natural Gas

The future reliability of the oil and natural gas infrastructures may be a challenge in the future. Many factors could affect the traditional reliability and security of the oil and natural gas transportation and storage infrastructure, including the following:

- Competitive markets in the natural gas industry are growing so rapidly that system use is increasing.

- The age of both oil and gas pipelines is a potential safety concern: most pipelines are more than 30 years old. Risk assessment and leak management programs are frequently used to help to determine when pipelines become unsafe, particularly in urban or sensitive areas.

- Compliance with environmental regulations increases operating costs in both industries. The oil industry also is driven to produce “greener” products.

- U.S. dependence on foreign supplies has increased significantly: more than 50% for oil and 13% for gas.

- Reduced investments in new technology and its applications are barriers to efficient operation and reliable protection of operations and the infrastructure.

- Both industries increasingly reduce costs through automation and downsizing. As these industries rely more on computers and automation, the possibility of a cyber attack increases.

- Concern over pipelines and production expansion has led to the NIMBY attitude. Permitting and siting issues are expected to grow in importance because of increases in oil imports, shifting population, and increases in the use of natural gas.

1.3.3 Challenges in the Energy Industry

The entire energy industry faces many significant challenges:

- Maintaining reliable energy delivery systems, while undergoing restructuring and change.

- Understanding the complexity and identifying the vulnerabilities of the emerging system and managing the inherent vulnerabilities cost-effectively.

- Preventing the spread of disturbances (either natural or man-made) to transmission systems to avoid widespread outages and long-lasting disturbances.

- Developing and implementing real-time control and communications systems to help to ensure a reliable supply of energy.

- Developing and implementing information security technologies to protect energy system information and communication systems from disruptions.

- Ensuring that our nation is protected against disruptions in fuel supply.

- Developing appropriate policies, incentives, and, where necessary, standards to assure the integrity of energy transmission systems.

- Ensuring that the energy industry's evolution enhances industry's competitive position in the world marketplace and increases our quality of life.

- Creating an atmosphere in which government and private industry share information to improve infrastructure assurance.

1.3.4 Ultimate Energy Industry Configurations

Recommendation of specific energy research areas depends in part on assumed results of rapid changes in the industries. That is, will restructured energy industries be a slightly modified version of historical vertically integrated industries or will they be horizontally integrated? One characteristic of a vertically integrated industry is that all controls, all control variables, and all system states are measurable and available to a central entity. The horizontally integrated industry is characterized by a high degree of uncertainty, and most services are acquired through the market. No position has been assumed for this report, and therefore some R&D recommendations are more appropriate for industry configurations than for others. As the recommended R&D topics undergo further study, specific "end games" for the restructured industries should be examined to identify the most relevant R&D activities.

Section 2
Threats and Vulnerabilities

Energy systems in the United States are normally reliable and economical. Energy companies can minimize the impacts of highly unlikely events, such as multiple simultaneous equipment failures at a single site. However, sabotage, terrorism, or a major natural disaster can inflict unprecedented damage.

Although U.S. energy companies have performed well, restructuring and competition have increased the stress on the energy system infrastructure, and it is uncertain how these systems would work under extreme circumstances. Therefore, both industry and government must investigate the likelihood of such potential damage, and, if warranted, develop ways to reduce risk, minimize damage, and mitigate the effects of outages.

The U.S. energy system is vulnerable to disruption and destruction from multiple threats and actions. Physical threats include terrorists and insiders, natural hazards, and accidents. Cyber threats originate from routine technical problems or from sabotage to information networks, energy management systems (EMSs), and SCADA systems.

2.1 Threats

Threats to the U.S. energy system arise from various sources, including hostile governments, terrorist groups, other organized groups or individuals, disgruntled employees, malicious intruders, natural disasters, accidents, system complexities, and dependence on other infrastructures. The U.S. Department of Energy (DOE) has documented more than 1,000 incidents against the U.S. energy system over the past 15 years; some supply disruptions have caused significant damage. In recent years, cyber incidents, including deliberate and accidental malfunctions, also have been documented.

Terrorists are not known to have caused any long-term energy outages in the United States. However, energy system components have been the targets of numerous isolated acts of sabotage. Several incidents have resulted in multimillion dollar repairs. For example, a 90-minute blackout that disrupted San Francisco on October 23, 1997, was attributed to sabotage.

Well-organized groups (perhaps working with insiders) could cause massive physical and cyber damage to our energy supply systems. These groups could damage the system so severely that major cities or multistate regions could suffer severe, long-term energy shortages. By carefully studying open-source information, such groups can increase their chances of causing major damage.

Cyber threats are rapidly increasing, as the industry becomes automated and interconnected, and more entities can access information that could be used to attack the system. While documented cases of insider attacks on computers are basically few, a knowledgeable insider has almost unlimited ability to cause problems, from bypassing access authorization to subverting systems. The rationale for an insider attack ranges from disgruntlement to financial gain and is the subject of much conjecture.

The Defense Science Board (DSB) concluded that threats to the national and defense information infrastructures include:

- Incompetent, inquisitive, or unintentional blunderers; mischief makers; and pranksters.
- Hackers driven by technical challenge.
- Disgruntled employees or unhappy customers seeking revenge for perceived wrongs.
- Criminals seeking personal financial gain.
- Organized crime seeking financial gain or trying to conceal crimes.
- Individual political dissidents attempting to draw attention to a cause.
- Organized terrorist groups or nation states trying to influence U.S. policy through isolated attacks.
- Foreign espionage agents seeking to exploit information for economic, political, or military purposes.
- Tactical countermeasures for impairing U.S. military weapons or command systems.
- Multifaceted tactical information warfare aiming to disrupt a major U.S. military mission.
- Large, organized groups or major nation states intent on overthrowing the U.S. government by crippling the national information infrastructure.

On the basis of validated incidents, the DSB concluded that some threats exist, while others are possible in the near future.

Threats can be “incidental” (or “inadvertent”) or “malicious” (or “deliberate”). Many threats (particularly complex threats) result simply from a lack of understanding about how things work or may work. As a result, malicious parties can exploit new vulnerabilities. Research can be a significant help in this area.

2.2 Vulnerabilities

The vulnerabilities that the energy infrastructures must face are described below:

- Vulnerabilities are created in the operating environment because of the rapid proliferation of industry-wide information systems based on open-system architectures, centralized operations, increased communications over public telecommunications networks, and remote maintenance.

- SCADA systems are not protected by encryption or authentication; however, they typically use proprietary message protocols and dedicated communication systems. Pressure to reduce costs is driving the industry toward open systems and shared communication networks. Data will be required from an increasing number of field devices, but competitive pressures will limit information security expenditures. SCADA systems are vulnerable because (1) the industry has not increased security measures in the configuration and implementation of commercial-off-the-shelf (COTS) hardware and software, (2) connections are made to other company networks, and (3) the industry relies on dial-back modems that can be bypassed. (These COTS systems may be more reliable than the customized versions, but their widespread use introduces new vulnerabilities.)

- The availability of information that can be used to identify vulnerabilities has increased, and much more is mandated by regulatory bodies to facilitate competition. In addition, tools are available for exploiting those vulnerabilities. Easy availability of information is a major concern to the industry.

- Advanced technologies, with inherent complexities, are rapidly assimilated.

- Infrastructure corridors (e.g., communications, electric transmission lines, pipelines) are being consolidated.

- The industry as a whole has not adequately addressed previously identified physical vulnerabilities of critical assets, such as control centers.

- Few technical and operational standards for specifications, system measurements, and codes of practice are in place.

2.2.1 Electric Power

The physical vulnerability of greatest concern to the EPS is a cascading failure. A cascade is the progressive failure of the system, as sequential outages of individual components result in widespread voltage collapse and system de-integration. When a large power system is stressed, cascades can be initiated by coupled failures of single components that, taken individually, represent minor problems. Cascades typically involve minimal equipment damage and are resolved within a few hours. However, when

significant damage to equipment occurs (e.g., 1998 outages in Auckland and Quebec), the time and expense of restoration increase significantly. The initiating events of modern cascading outages have been accidental failures during infrequent periods of high system stress or unusual operating conditions. Deliberate attacks under such conditions, however, would have the same effect. Periods of high system stress will likely become more frequent as the restructured competitive electric market develops. Other physical vulnerabilities of concern include control centers and substations, although certain generation facilities and transmission lines also are of concern.

Deliberate attacks on the integrity of the grid require coordination. Because more information about electric power grids is available, it is possible for knowledgeable individuals to coordinate devastating attacks by targeting a few selected components (e.g., control centers). It is thus important to study countermeasures to such attacks. The nature of power systems means that effects multiply over long distances very quickly.

SCADA systems are among the most attractive cyber targets to disgruntled insiders and saboteurs intent on triggering a catastrophic event. Because of the exceptional growth of information system networks needed to interconnect business, administrative, and operational systems, intruders could disrupt them easily by accessing a SCADA system and modifying the data used for operational decisions, the programs that control critical industry equipment, or the data reported to control centers.

2.2.2 Oil and Gas

Both the oil and the gas infrastructures are vulnerable targets. Their systems are extensive and generally accessible to other utilities — and often to the public. Protective fences and security along all production, transportation, and processing points are not feasible because of costs.

These highly complex infrastructures rely on production and gathering, processing and storage, and transmission and distribution to move oil and gas and to the marketplace. These infrastructures are extremely capital-intensive; a single oil platform can cost $50 million or more, with deep-water platforms costing 10 times that amount. Tankers can cost millions of dollars — liquefied natural gas (LNG) tankers are the most expensive vessels, except for military ships. Construction of transmission pipelines can cost up to $1 million per mile, not including the compressor or pumping stations, which can exceed $40 million and are required approximately every 50 miles. Petroleum refineries, gas processing centers, tank farms, gas storage fields, odorant facilities, and distribution systems are other costly investments.

These infrastructures are difficult to protect. For example, the United States has enough gas pipelines to encircle the earth more than 7.5 times. Security measures, such as fences and guards, are not economical because of the large area in need of protection. Currently, no mandatory or voluntary security standards (except for LNG facilities) exist for these infrastructures nor is there a regulatory body that oversees security issues.

Well-heads, gathering pipelines, waterborne vessels, control centers, tank farms, transmission lines, pumping stations, compressor stations, refineries, gas processing centers, city-gate stations, distribution pipelines, LNG facilities, and odorant facilities also are vulnerable to threats. The degree of vulnerability depends on the importance of each component to its respective infrastructure and the amount of redundancy. For example, well-heads are less vulnerable than other components because of the large number of wells and the ability to extract oil or gas from substitute wells. City-gate stations are highly vulnerable because they are few in number; however, they are important because they connect to distribution pipelines.

One of the infrastructure's greatest vulnerabilities is the nation's dependence on foreign oil. The 1973–1974 Arab oil embargo made it obvious that oil shipped from an unstable area halfway around the world can be cut off at will, priced almost at will, and cause major economic hardship. Also, in 1979, a 1% reduction in the availability of oil worldwide during the Iranian revolution triggered long lines at gas stations and a 120% price increase in the United States. Despite these major supply disruptions (and the Gulf War), the nation is at an all-time high (more than 50%) in depending on foreign oil.

As in the electric power industry, SCADA systems used in the oil and gas industries are subject to electronic intrusion. If accessed, information could be manipulated or control programs could be modified. Under certain circumstances, a hammering effect could be induced in pipelines, possibly leading to breaks. Similarly, remote-controlled pressure regulators could be manipulated to cause over- or under-pressurization and explosions. More research is needed to determine the feasibility of such attacks.

To minimize costs and increase efficiency, many companies are expanding their automation and networking systems dramatically and linking their control, administrative, and business information systems. Cyber threats represent unique vulnerabilities to these infrastructures. As these systems move to open-system architectures that use standard protocols and interconnected systems, hackers find it easier to access most systems because they are based on personal computers. Various Internet forums provide "cookbooks" that explain how to break into systems; some even provide access passwords. As systems become highly interconnected, access to multiple systems across multiple computers would become easier, which would increase the effects from hackers who access the system.

Section 3
R&D Topics and Activities

This section describes several research and development (R&D) topics considered top priorities for federal support. Each topic is discussed in a separate section, which describes the goals and challenges for the R&D, the rationale for the research and its desired results, and an estimate of the timeframe and resource requirements for the research. The following topics are addressed:

- Electric Power Systems

    1. Real-time control mechanisms
    2. Analysis of scale and complexity
    3. Vulnerability assessment
    4. Information assurance and cyber security
    5. Emergency response and recovery information technologies
    6. Transmission and distribution technologies
    7. On-line security assessment
    8. Dispersed generation and backup infrastructures

- Oil and Natural Gas Systems

    9. Critical consequence analysis
    10. Decision support systems
    11. Physical protection assessment
    12. Multisensor and warning technologies
    13. Emergency response capability enhancement
    14. Cyber protection enhancement

- Joint Topics

15. Evaluation of policy effects

16. Institutional barriers

17. Infrastructure interdependencies

All of the R&D topics discussed in this section are worthy of federal assistance to improve energy infrastructure assurance. Substantial industry efforts are underway for some research topics; additional federal support is necessary and appropriate to achieve timely results and provide for energy infrastructure assurance. Some of the research topics have primary objectives in addition to infrastructure assurance. In those instances, federal support on the infrastructure assurance aspects is encouraged. In other cases, the proposed research is pioneering, so the federal government must initiate this effort. Industry presumably would participate and contribute financially as the research proceeds.

Some R&D topics listed in Sections 3.1 and 3.2 are partially relevant for the oil and gas infrastructure and vice versa. Joint (interdependency) topics listed in Section 3.3 apply entirely to both the electric and the oil and gas infrastructures.

3.1 Electric Power Systems

3.1.1 Real-time Control Mechanisms

Description

Although utilities provide on-line control of the major features for operating the electric system, man-in-the-loop operator control, automated control for limited functions (e.g., automatic generator control), and locally activated control for protection are typically combined. In the future, increases in the interconnected complexity of the power system, the introduction of new distributed resources (e.g., generation, storage, load control), and increased stress on existing grids will make real-time automated control a necessity. Coordinated control over larger portions of the grid will be required (coincidentally being mandated under Federal Energy Regulatory Commission [FERC] regulations). Dramatic enhancements in technology and its implementation will be needed to ensure reliable service.

Currently, the only available control is generation set-points (real power and voltage). A more flexible alternating current (AC) transmission system is necessary because in the future generation control may not be available and the market, whatever it is, works best with an unconstrained delivery system. The current control philosophy is assessment and avoidance; it must be replaced by identification and control. However, control methods are needed that can tolerate a large degree of uncertainty and complexity. Methods that allow control on the basis of data rather than on models are needed because it is unlikely that sufficiently complex and/or detailed models would be available.

Several topics included in the suite of technology R&D required for real-time control have been addressed because of their importance. These topics include on-line security assessment, advances in computational algorithms, advanced high-power electronic switching technology, and approaches for dealing with complexity. Additional development is needed in four areas, which are described in greater detail in the following subsections.

Instrumentation and Monitoring for Distributed Control. Monitoring is unique in its relation to real-time system control in that the required decision making is inextricably linked to the quality and timeliness of the information received. "What cannot be measured cannot be controlled" is the basic axiom of decision and control. Monitoring includes systems for collecting time-synchronized data gathered from disparate points in the system, as well as tools to extract and disseminate the data for a given application. This definition implies that raw information, such as that obtained from the terminals of a transducer, is not very useful to the decision maker.

Applied research and advanced technology development are required to upgrade these large-scale data collection systems to the level required for implementing real-time power system control. The objective of this research would be to design hardware and software systems that can accurately collect and manage large data streams that emanate from geographic locations throughout the grid.

Analysis and Computation for Large-scale Systems. Production and delivery of electricity are data-intensive industries. Real-time control requires massive data sets in addition to those used by electric utilities.[3] Advanced visualization techniques, user-friendly human/machine interfaces, and expert systems must be developed to process this volume of information. Basic and applied research, advanced technology development, and proof of principle and validation can produce software systems capable of conveying complex detail and intricate dependencies to utility engineers and operators.

Advanced Control Methods. As more large-scale control devices are developed to enable systems to operate closer to theoretical limits, the role of stability control systems significantly expands. The control of future large-scale devices affects the behavior of the system. Proper controls produce beneficial results; whereas improper controls result in disaster. Therefore, the control system must be reliable and resilient as operating conditions change. Meeting these needs requires advancements in, for example, communication and coordination between central and local controllers, coordination between different local control stations, robust control theory of large-scale systems, and intelligent hierarchical supervision of local controllers. The ideal real-time stability control structure is decentralized; that is, most decisions are made locally, which minimizes dependence on communications. Communicated information and control at

[3] As used in this report, "utility" refers to the system operator, generator, or supplier in the restructured environment.

different hierarchical levels enhance the performance of the local control systems and ensure optimal system-wide control.

Proper disposition of the themes covered by this topic requires all types of research, especially basic research. The product of the R&D conducted under this topic will be a new body of control theory specifically developed for large-scale systems, but applicable to other large-scale nonlinear systems (e.g., the stability of space structures).

Decision Support Tools. Decision support is a critical element for real-time control architecture. Like any other critical infrastructures, the EPS relies on human engineers and operators to use good judgment to ensure reliable service. They need the best tools available to take informed actions to manipulate and protect the bulk grid.

The decision support architecture for real-time control should be both distributed and hierarchical. In general, modules of the decision support system should be physically located with individual components, major component groups, substations, regional offices, and the central distribution center. Reasoning requirements and the scope of influence increase for modules as they progress up the hierarchy, from the component groups to the distribution center. Component modules "reason" about their respective components and pass conclusions up the hierarchy or request that information be sent down the hierarchy. At the other end of the hierarchy, the scope of the central distribution decision support module includes the entire distribution system and, for the most part, addresses issues involving the high-level power distribution network.

This topic requires a broad array of research activities from basic research to advanced technology development and proof of principle and validation. The new hardware and software systems will enable real-time control for people charged with seeing that the system operates continuously and efficiently.

Goals and Challenges

Instrumentation and Monitoring for Distributed Control. A set of fully compatible EPS models is needed to coordinate control over broader areas and to distribute intelligent real-time control into the distribution systems. Information across traditional organizational and topological boundaries would be shared in real time. The EPS models need protocols for data acquisition, communication, storage, access, and dissemination. Important operational information must be available in a distributed manner. Both local decisions and control actuations must lead to optimum use of emerging technologies for distributed resources and stability enhancement, but, in particular, to enable control during emergencies.

Measurements must be made with timing accuracies that have not been required in the past. The system must provide much larger volumes of information, sufficient to characterize events at higher control levels, both locally and collectively, as they are developing, progressing, or being analyzed in detail. Better optical measurements of EPS behavior are required. They must provide temporally precise data at costs comparable to,

or lower than, those of conventional transducers. Measurement devices that enable adaptive monitoring, by using complex pattern-based event recognition filters and triggers, are also required.

The large amount of information to be gathered at distributed points in the grid requires very high bandwidth communication systems. Although early wide-area measurement systems can require only episodic communication when events occur, real-time communication should be anticipated and necessary bandwidth secured. A significant investment can be required for communication systems; therefore, methods and algorithms should be explored that reduce or condense measurement information (such as wavelets). Consistent with communication requirements, new protocols are probably necessary to meet progressive and expanding needs in this area. Finally, the means for coordinating information exchange in highly dynamic circumstances are required.

Analysis and Computation for Large-scale Systems. Current efforts in this area focus on developing methods for extremely fast simulation of potential contingencies, starting from a known operating point (typically the current operating point). Known as on-line security assessment (OSA), this area of research requires accurate models of the system under study. As with all large-scale systems, it is challenging to develop models with the degree of accuracy required to result in meaningful OSAs. It is essential that "measurement-based" methods are used with "model-based" methods such as OSA. The effort in this area must focus on measurement- and model-based methods to (1) compute the necessary stability indices more quickly than is possible at this time and (2) accommodate uncertainty in system analysis.

A stability index is a metric that defines the ability of the bulk power grid to remain interconnected, given the introduction of a known disturbance. The development of one or more good indices gives operators new tools to use in making switching decisions or manipulating line loadings. Uncertainty is a factor in all dynamic systems, but the magnitude of the uncertainties in large-scale systems presents unusual challenges in signal processing, simulation, and other types of analysis. Consider modeling a refinery with thousands of dynamic elements — a challenging process. The interconnected power system has thousands of assets, such as a nuclear power plant, with at least the level of sophistication of a refinery. With only a slight uncertainty in each modeled element, the magnitude of the aggregate uncertainty often makes the analysis meaningless.

New effective paradigms are needed by which the results of complex, large-scale computations that involve great uncertainty can be meaningfully conveyed to operators and others in an intuitive and comprehensible manner. For example, newer and better indices of the system's performance under expected and/or anticipated conditions may be warranted. However, more effective means for conveying this information may require significant additional research and experimentation.

Computationally robust and verified solution methods are needed for large-scale systems. These methods must not only consider uncertainties in the computation, but also uncertainties in the data and the models.

Advanced Control Methods. Although an abundance of scientific literature in control theory is available, the control of large-scale systems is especially challenging. To achieve the principal goal of this effort, it may be necessary to extend existing control theory in new directions or develop new approaches to better address some of the unique challenges of controlling a highly dispersed structure. The effects (1) of one actuator on an actuator hundreds of miles away, (2) of losing a control actuator, (3) of losing an information link critical to controller operation, and (4) of changes in power system topology on a control algorithm must be taken into account in ways never before conceived.

Robust control theory refers to control theory that deals with maintaining effective control in an environment of changing system parameters. In the EPS, grid topology constantly changes, as lines, generators, and loads are switched in and out of service. One of the goals of this research to advance robust linear and nonlinear control theory to reduce the grid reserve margins.

Finally, implementation of a decentralized control scheme requires the development of methods for dealing with degraded knowledge or power system capability. An autonomous controller must not fail because of a lack of knowledge of parts of the surrounding system. Methods must be developed to ensure that this type of information system failure does not form a “rogue” controller that acts contrary to goals of the remainder of the interconnected control hierarchy. This problem, in the form of “over-reaching relays,” played a role in the 1996 western U.S. outages. In effect, the team proposes to conduct research on revamping, upgrading, and refining the conceptual design of the relay and control structures of the system.

Decision Support Tools. The reasoning element is the heart of any decision support module. It transforms data into information, analyzes data and information, draws conclusions, solicits information from other modules and from the system operators, and develops recommendations. The goal of this research is to develop technologies required to implement a functional reasoning element for decision support on a large-scale, widely dispersed system such as the electric power grid.

The reasoning element must use some form of artificial intelligence (AI). To date, applying AI tools to power system problems has had mixed reviews. AI-based tools have been applied only to well-defined problems, such as processing alarms. New AI tools are needed to aid human operators in the overall decision-making process. A key element is developing multiconstraint optimization tools that accommodate all the relevant objectives for operating a power system, in particular, situationally adaptive optimization tools.

An additional goal is to develop autonomous agents for reasoning and optimizing system operations. These agents would operate at the higher levels of the control hierarchy and assist in the decision-making process for mundane, but critical, system performance measures. The logic for these autonomous agents would extend down to the delivery level, where they could assist operators with complex circuit diagnostics. They could help to minimize customer outages (e.g., through adroit circuit switching), maximize asset use, and improve many operational procedures currently carried out ad-hoc.

Rationale for the Research and Desired Results

Instrumentation and Monitoring for Distributed Control. Advanced instrumentation and monitoring systems, including the data systems that support their effective use, require vital R&D to enable the required greater utilization of the existing electric system (i.e., providing information essential for operating at inevitably lower reserve margins, for prompt avoidance of cascading events, effective management of emergencies, rapid recovery from major events). The degree to which power system reliability can be operationally managed depends on instrumentation and monitoring. On-line reserves increase the inertia of the system, which makes it more stable in the presence of disturbances.

Analysis and Computation for Large-scale Systems. Another reason the United States maintains significant capacity reserves today is that on-line information cannot be used effectively to calculate stability margins online. The computational challenge is too great for conventional algorithms and workstation platforms. While computational capacities continue to increase, work needs to be done to develop more effective algorithms and methods for computing stability indices, particularly for increasingly complex systems. Also, significant evidence shows that present models do not accurately predict power system behavior during stressed conditions because of assumptions made in the models and inherent nonlinearity exhibited during stressed conditions. In addition, no methods incorporate uncertainty in on-line dynamic stability tools. Such advances are essential for both preventing and recovering from significant power system outages.

There is a need for better understanding of uncertainty. Low-probability, but high-damage, events are most important for infrastructure assurance analysis, but traditional analysis methods do not effectively capture these effects. Thus, not only are risks present in using the system, but they also are not apparent. How close we are to safe limits depends on knowing where we are and what the limits are.

Advanced Control Methods. Trends in technological and infrastructural development have changed the landscape of power system topology and control. These trends enable greater use of distributed elements of the system for control (e.g., development of flexible AC transmission system devices and distributed load control), while also increasing the need for projected widespread implementation of distributed generation. New control methods are essential for enabling the use of such

devices. With these control systems and devices (systems of devices), reliability can be managed to minimize the effects of undesirable incidents or events. These devices increase the options that operators and their automated agents have to prevent or manage a potential outage. Recovery also is substantially enhanced if an outage occurs.

Decision Support Tools. Substantial improvements in the type, quality, and quantity of information available for operating the increasingly complex power system in real time would be lost if the information could not be used to make prompt, accurate decisions related to control. The massive amounts of information processing, calculation, analysis, and reasoning required to manage the power system would overwhelm present operators if they did not have additional automated decision support tools. If the operators or yet-to-be-developed automated agents are not able to make decisions with confidence and at the appropriate time, many operational options will remain beyond implementation, and advances in each of the areas above would have limited effect. Decision support tools being developed would be of particular value for diagnosing problems and would be of immense value during emergencies, when most control rooms overwhelm operators with information (much of it irrelevant).

Timeframe and Resource Requirements

Because of the complexity of the EPS and because the United States relies on it for our entire well being, the development and demonstration of systemic technologies are long, frequently expensive processes. The electric power industry is the most capitalized in the nation and has equipment lives often measured in decades.

Table B.1 provides estimates of the timeframe and resource requirements for developing real-time control technologies.

3.1.2 Analysis of Scale and Complexity

Description

Scale and complexity primarily involve issues and vulnerabilities caused by the sheer size of the interconnected transmission grid, along with the increasing use of more sophisticated components and technologies within the grid (for example, an increased use of power electronic components). In almost all cases, a larger grid with more technologies in use leads to more complex and less intuitive situations. The objectives of an R&D effort in this area are as follows:

- Develop a better understanding of the stability characteristics of very large systems, which integrate economics, physical energy delivery, communications, and computation.

Table B.1 Estimated Timeframe for Developing Real-time Control Technologies

Technology Area	Timeframe	Cost[a]
Instrumentation and Monitoring for Distributed Control	3 yrs: first field test of WAMS	5
	5 yrs: first incorporation in operator-assisted control	20
	10 yrs: first use in large-scale automated control	60
	15 yrs: first coordinated use at multiple scales	45
Analysis and Computation for Large-scale Systems	3 yrs: near-real-time stability computation for 1,000-bus system	15
	5 yrs: 10,000-bus system	25
	10 yrs: incorporation of uncertainty in on-line calculations	60
Advanced Control Methods	3 yrs: next-generation architectures detailed	8
	5 yrs: first subcomponent field trials	20
	10 yrs: first field trials of full multilevel hierarchical systems	60
Decision Support Tools	5 yrs: first field trials of AI tools in control room	10
	10 yrs: first automated agents in control rooms	30
	15 yrs: first coordinated intelligent control optimization tools at multiple scales	45

[a] Costs are estimated in millions of U.S. dollars.

- Study countermeasures to avoid or mitigate malicious control.
- Study technologies that might reduce, or help to cope with, complexity.
- Develop tools for very large-scale computation.
- Study large network interactions, voltage collapse, and network security.
- Study the effect of uncertainties and changing conditions on systems.
- Study the effect of complexity and scale on human behavior.

Complexity need not imply numerous components (though power systems have that challenge, too). Even very simple nonlinear systems can be difficult, if not impossible, to analyze and can demonstrate very complicated (i.e., chaotic) behavior. Local linearization (or piece-wise linearization) enables treatment of nonlinear systems as linear systems over certain operating regions where the system is "well behaved." However, characterization of the appropriate operating regions is not well developed and varies on the basis of changing parameters that characterize the system. For instance, as stress on the system increases, nonlinearities are expected to become more important in characterizing system behavior. Compelling evidence shows that months after the massive outage in the western U.S. grid on August 10, 1996, transmission planning staff still could not simulate the observed behavior even after substantial deviation of many model parameters from their expected values. Traditionally, nonlinearities have been relatively unimportant because the system was "overdesigned" and rarely stressed to its operating limits. That situation is not likely to persist.

Another topic worthy of attention is uncertainty in power system operations and reliability. At present, probabilistic methods are not used much in operating the grid. For example, probabilistic methods are not used for assessing the proximity of the present operating condition to unstable operating regimes or for conducting on-line adaptive risk management. In a competitive market, efforts to increase equipment use and life would become even more intense, which would affect the probability of component failure and potentially increase the risk of cascading outages.

Goals and Challenges

The goals and challenges in the area of scale and complexity are as follows:

- Develop a more complete understanding of all the threats and failure modes that can occur in a power system as a result of increased system complexity.

- Develop the tools necessary to mitigate the effects and to understand and prevent problems in complex systems.

If successful, this research would reduce infrastructure vulnerability by addressing the core of one of the more fundamental vulnerabilities of a large interconnected system. It is important that designers, operators, and policy makers understand the issues brought about by complexity. A thorough understanding of these issues would result in:

- Development of policies, procedures, and standards that simplify rather than increase complexity.

- Designs that reduce adverse effects, leading to systems that are inherently more robust and less likely to fail.

- Ability to deal with large-scale systems, which would ultimately reduce costs and improve societal economic welfare.

- A system less vulnerable to deliberate attacks or intrusions, which would reduce the possibility of highly disruptive behavior.

- A reduction in the number of outages and system events, which is timely because disruptive events are expected to increase as a result of deregulation and the pressures to operate more economically. The recent clamor from the outages in Auckland and the western United States in the past two years is an example.

In short, this work is important not only because it will lead to a more reliable grid, but also because it will be capable of promoting efficient competition and improving overall societal welfare.

The main strategy recommended for attaining these goals is an organized research effort that addresses the issues of complexity in general, with specific applications to

complexity in power systems. The effort should encompass the following project categories:

- Conduct research on understanding complexity as a discipline of its own. A general understanding is needed of complexity and what it does to systems; principles by which one can deal with complexity in real time; a generic taxonomy of complexity issues; and how dynamic effects, uncertainty, size, interconnectivity, and other factors contribute to the multidimensionality of complexity.

- Perform research on the human aspects of complexity, i.e., general principles and experimental results on how humans cope with complex situations, both when given time and under real-time conditions.

- Perform research on the tools needed to address, understand, and conquer complexity. Tools to monitor power markets and grid operations for evidence of manipulation are also needed.

- Apply the principles of complexity theory to develop tools that address the specific needs of a power transmission system. Other dimensions of complexity in power grids include safety, nonsimultaneity of results, uncertainties due to weather, and more.

Rationale for the Research and Desired Results

When large nonlinear systems are assembled, many patterns of behavior are poorly understood, which can lead to areas of erratic behavior and resulting failures. Modes of operation that do not exist in simple systems can be implemented as systems become complex.

The electric power grid is becoming more susceptible to disruption for financial gain. It is possible to create problems deliberately and then hide behind complexity. The topic of sophisticated, deliberate attacks on the power grid has not been fully explored. Furthermore, unsophisticated attacks on complex systems should not be ignored, because the more sophisticated the lock, the more susceptible it may be to primitive attack. It is important to understand all vulnerabilities.

The inability to determine or comprehend the overall status of the grid in real time is a problem. This aspect of complexity involves the abilities of humans to assimilate and process information about unfamiliar situations. Recently, many problems (including more than one blackout) have been attributed, at least in part, to the inability of an operator to obtain a sufficiently comprehensive “picture” of what is happening.

Timeframe and Resource Requirements

Research on timeframes and resource requirements is more fundamental, but no less important, than some of the other topics. The budgetary and possible project recommendation in this area is organized into several possible project categories:

- An immediate intense three-year effort aimed at understanding how deregulation may (or may not) increase system complexity, along with an understanding of important new issues that result from deregulated operation. Most important is an understanding of the interactions between networks and markets, which should include market power considerations and dynamic effects.

- A five-year effort with strong input from theoreticians and others with a goal to improve our understanding of complex systems in general. This effort would require approximately $2 million per year.[4]

- A five-year effort to understand human interfaces and how humans deal with scale and complexity when under pressure. This effort would require approximately $3 million per year, including some funding for human factors experimental work.

- A five-year effort to understand the complexities in the power grid itself, looking for situations where complexity can lead to fundamental changes in the behavior of the system. This effort can be integrated with efforts aimed at understanding the present and future grid. Suggested budgets would have to be coordinated.

- A five-year effort, coordinated with other groups, to develop computational capabilities for dealing with uncertainty. Suggested budgets would depend on other efforts.

- An effort specifically targeted at understanding uncertainty and all the ways in which uncertainty makes a system vulnerable, along with ways for mitigating the effects of uncertainties. This effort would require approximately $4 million per year.

3.1.3 Vulnerability Assessment

Description

The EPS is being restructured to a market-based environment. It is likely that centralized planning and coordination, as practiced by utilities in a regulated environment, will change. To remain competitive in the future, utilities need to control costs, so they may need to operate with lower safety margins. Traditional safety margins, such as higher generation and transmission reserve capacities, typically built into electric systems in a regulated environment, may not be as large after restructuring. Consequently, alternative safety margins may be needed to prevent an increase in the vulnerability of the electric grid or a decrease in its ability to respond to, and recover from, threats.

To date, a comprehensive evaluation has not been performed of the vulnerabilities/threats to the EPS in a restructured environment and with resulting consequences or impacts. Although vulnerability and threat issues have been identified

[4] Some reviewers believed this cost estimate should be increased substantially.

and some consequences have been quantified, a comprehensive evaluation, including significant technical analysis, has not been conducted. Such an evaluation would examine vulnerabilities to sabotage, acts of terrorism, system complexities, and acts of nature.

A careful study of the potential future architecture and structure of the electric industry is particularly timely and important. Incentives for utilities to invest in reliability measures (particularly R&D) are unclear, and investment has dropped precipitously in recent years. In the emerging, competitive market, it is not clear that anyone has responsibility for developing new approaches and technologies for enhancing reliability, particularly if implementation is required at the system level.

Competitive markets are particularly responsive to changes in the environment in which they operate and are very efficient at moving to a new equilibrium point. However, they are generally poor at anticipating major low-probability shifts in the underpinnings of that market. Understanding how such changes can influence grid reliability is important because it can direct R&D to help ensure that a prudent array of technologies and policies is available.

This evaluation would provide useful information on a national or large regional scale for assuring a reliable electric power system. It would also analyze systems under extreme or highly unusual conditions that do not arise during normal business activities. This R&D is not intended to replace or interfere with risk management evaluations performed at the individual utility level.

The purpose of this analysis is to identify system vulnerabilities and strategies to prevent large-scale outages and mitigate consequences from them. It will also identify ways to encourage utilities to make the necessary investments, such as increased generating and transmission reserve capacities, in a deregulated environment to achieve national security goals. The federal rules separating production and delivery create an environment in which tight integration of planning is less likely. The government’s role in offering incentives to encourage utilities to make these investments in a competitive marketplace will be examined. Possible incentives the government can offer are cost sharing, tax breaks (unlikely, but possible), policy/regulatory changes, technical support, etc.

Goals and Challenges

The goals and challenges associated with evaluating current and future EPSs include the following:

- Identifying and evaluating strategies for preventing regional outage incidents and mitigating consequences.
- Identifying and evaluating strategies for recovering from incidents.
- Assessing the reliability and maintainability of key EPS components and their relation to the system as a whole.
- Assessing the value of new technologies that could improve the reliability of the power system.
- Assessing local and overall benefits and costs of changes to the system as restructuring transforms it.
- Evaluating the vulnerability of the system to disruptions in fuel supply and assessing the need for alternative fuel or fuel switching generation technologies that could enhance system reliability.
- Identifying and evaluating the effects of alternative electricity restructuring scenarios on the transmission and distribution systems.
- Identifying and evaluating incentives, such as cost sharing, tax breaks, policy/regulatory changes, and technical support, to encourage utilities to invest in technologies and procedures to protect critical components of the electric grid and achieve national security goals.

Rationale for the Research and Desired Results

A comprehensive assessment of the vulnerabilities or threats to the EPS and the resultant consequences or impacts at national, regional, and company levels is needed to aid in decision making concerning research, capital investments, and changes in regulatory requirements and operational practices. A framework and methods are needed for conducting these assessments. Some of the methods can be developed as part of other research recommended in this report, but additional analysis techniques are required as well.

The analysis would also identify and evaluate options to address grid vulnerabilities. Furthermore, because of deregulation in the electric utility sector, government incentives that encourage utilities to invest in the EPS to help achieve national security goals would be identified and evaluated. This system evaluation could develop into a top-level analysis that guides other tasks.

Timeframe and Resource Requirements

The overall objective of these assessments is to improve risk management decisions. To meet this objective requires the following actions:

- Developing systematic and consistent estimates of the vulnerabilities and threats.
- Quantifying the potential consequences or impacts.
- Evaluating the effects of actions to prevent, mitigate, and manage incidents and to aid in recovery.
- Evaluating the need for government incentives to encourage utilities to invest in the electric grid to address vulnerabilities.
- Estimating the uncertainty and the effect on electricity prices for all of the above analyses.
- Developing decision frameworks to incorporate the above information and assist in risk management decisions.

The research required for this topic would be an ongoing effort to develop and improve modeling and analysis capabilities for evaluating regional or national electric power systems. Required funding is estimated to be $35 million through 2010.

3.1.4 Information Assurance and Cyber Security

Description

Electric utilities depend significantly on information and telecommunications systems. Historically, many utilities have installed and maintained their own dedicated communication systems. Often, they had separate computer networks for administrative and operational systems. Operational systems (e.g., supervisory control and data acquisition, SCADA, and energy management systems [EMSs]) have typically been segregated and closely monitored; interconnection with other computer networks has traditionally not been allowed. Utilities typically invested in redundant telecommunications systems to ensure reliable information systems for operation. In general, utilities have not experienced information attacks. However, deregulation provides motivation for financial gain and changes in the sophistication of cyber threats, as well as development of information warfare as an international threat, increase the need to ensure appropriate measures are used for information assurance. Unfortunately, utilities, though long used to dealing with natural disasters or random physical assaults on facilities, are not prepared to deal with cyber threats, particularly from structured adversaries (few infrastructures are).

Electric utilities, in particular, depend on large amounts of real-time information typically associated with their SCADA systems. Current SCADA systems use open

protocols (such as the Inter-Control Center Communications Protocol [ICCP]) and a large variety of other protocols (both open and closed) for SCADA communications. Trends to use open systems and protocols, as well as intelligent (computer) electronic devices at field equipment sites (and in equipment itself) increase the potential for inappropriate access. However, the undetected interception and modification of SCADA signals would typically require extensive knowledge of the domain. Currently, encryption is not used in electric utility SCADA systems (or in essentially any other operational elements) nor is authentication commonly used. Information security typically has relied on obscure protocols and the need for considerable domain knowledge.

In addition, a new age of directed energy weapons (such as high-energy radio frequency [HERF]) is entering service and can, quite literally, be built with readily available parts and designs available over the Internet. Few evaluations of the effects of these weapons on electrical equipment have been performed. Research and development therefore focused on seven areas:

- Threat assessment and risk management tools specific to the electric power industry;
- Large, geographically disperse information systems;
- High-security SCADA network systems;
- Efficient, adaptable encryption;
- Robust authentication and authorization;
- Network intrusion detection for high bandwidth communications; and
- Evaluation of the sensitivity of electric power equipment and facilities to directed energy weapons.

There is a significant need to pursue additional efforts in institutional topics related to raising awareness and operations security in each of these seven areas described in greater detail below.

Threat Assessment and Risk Management. The electric power industry is unique in its size; it was constructed as an amalgamation of many diverse and independent stakeholders and relied on legacy systems. These characteristics, together with the current environment of deregulation and centralized control, are creating a situation in which EPS operators and planners are making decisions based on regulatory and economic constraints without access to knowledge of the vulnerability these decisions may pose to the infrastructure. Information systems are a vital part of the operations for the power grid. In the past, the industry accommodated risks according to generally accepted threats and vulnerabilities. Unprecedented institutional change, accompanied by continuing technical change, leaves many in the power industry without

an effective basis for making risk management decisions concerning information assurance (and perhaps other security issues).

Significant research is needed to develop threat assessment and risk management tools to help designers safely move the electric power industry into a more interconnected, market-based system. As the industry begins to understand the basic principles of these areas, applied research, technology development, and validation work will be required to adapt existing technologies to this specific domain.

Large Systems Analysis. The electric power grid is a very large, geographically dispersed system. With the move toward deregulation, the interconnectedness and interdependence of widely separated subsystems increase. To ensure the stability of this system in the face of faults, cyber attack, or coordinated physical/cyber assault, the entire system must be characterized and well understood. This information is critical to designing a fault-tolerant, robust power grid.

The EPS combines physical (power generation, transmission lines, etc.), logical (control circuits, automated breaker tripping, etc.), and information systems. Research is needed to understand this complex system, including distributed information assets and coordination and security of such a widely dispersed network of information assets. Models and simulation systems, which currently represent subsections of the grid, must be expanded to keep pace with deregulation and deployment of new technology.

In this area, both basic and applied research activities are needed. As models and tools are developed, a proof-of-principle and validation stage would be required. The outcome of this research effort should be new models, simulation techniques, integrated attack models, and planning/design tools. The tangible outcomes would include a better understanding of this complex system; a heightened awareness of the interdependencies; and a more efficient, reliable, and robust national power grid.

High-security SCADA Systems. SCADA systems handle the measurement and status information to allow decision making at the control center; manage control signals that actually set the operating parameters for generation; open and close breakers in the distribution system; return status information to the EMS; and allow for remote monitoring of equipment. The SCADA network transmits command and control information to remote subsystems. Often, the remote system does not verify the authenticity or validity of the control signal; the command is simply carried out. In the nation's EPS, the importance of providing secure communications for SCADA cannot be overemphasized.

Research into high-security SCADA architectures should be primarily applied with a strong validation phase. The result of this research will be varied and will include design guidelines and tools, models, test and evaluation tools, and possibly new protocols, encryption deployment, and authentication and authorization systems.

Efficient, Adaptable Encryption. Because utilities manage vast amounts of temporally sensitive information and at times must execute control functions in milliseconds, they have been reluctant to use techniques that might either increase potential latency in the data reception or unnecessarily complicate communications. The frequent use of vendor-specific protocols also has prevented the industry from adopting methods such as encryption, which can have high overhead requirements in terms of signal processing. Utilities do not want to use methods that slow operational communications (particularly when they are trying to increase their use of existing assets). However, there may be significant benefits from developing encryption technologies that could be used with minimal downside effects on operations. In the absence of obscure protocols (now being phased out), encryption may be one of the few ways to increase barriers to interception and/or intervention in communication of temporally sensitive information. The real challenge is to develop a cryptographic system that meets the industry's requirements.

Robust Authentication and Authorization. In the context of general information assurance, authentication is the process of confirming the identify of an individual or a system. For this discussion, authentication is the binding of a command or action to the entity or person issuing the command. In other words, authentication is the mapping of electronic actions to the person or system initiating those actions. Authorization is the process of establishing whether an authenticated entity has permission (authority) to carry out a specific action.

Research — basic and applied — is needed to develop and deploy strong authentication and authorization controls to both the SCADA and information networks deployed in the electric power industry. Because of the criticality of the systems involved, authentication and authorization must be hardened to tolerate faults and must not provide choke points for denial of service (or other) attacks. In an EPS, a mistaken denial of timely access can be almost as damaging as allowing unauthorized access.

Intrusion Detection. Detecting probes, penetrations, and attacks on an information system is critical for system security. Probes and attacks must be detected quickly to trigger a response, and penetrations must be detected quickly to initiate mitigation and recovery efforts. Intrusion detection must be efficient and accurate. The price for signaling a false alarm in a real-time control system could be quite high. Because of the high bandwidth and wide variety of communication types and protocols, intrusion detection is a very difficult task for the electric power industry. In addition, mitigation and recovery measures must be consistent with the necessary functionality and reliability of the EPS mission; that is, provide a reliable source of electricity.

Ongoing research in intrusion detection, mitigation, and recovery could be used as a springboard for work specific to the electric power industry. Applied research, technology development, and validation are required (more fundamental research may be necessary to address specific needs related to real-time system operations).

Directed Energy Weapons Countermeasures. Plans for building HERF weapons sufficiently powerful to disable an automobile or a computer from a distance are easily available. The vulnerability of the electric power grid to both random and coordinated HERF attacks must be assessed. If the grid is found to be vulnerable, research into ways to protect both the information systems and critical electric system elements (breakers, transformers, reclosers) should be initiated.

Research to assess the threat and viability of HERF weapons against the EPS infrastructure is a logical first step. The outcome would be a general, high-level assessment of vulnerability that outlines protective measures. This initial work would lead to focused R&D and testing of various facilities and equipment. Guidelines for facility design and security would be developed. More robust technology approaches to shield the system from such attacks could be developed if warranted. Mitigation and recovery plans must be augmented to include a response to this type of attack. (This research also should accommodate the expected increase in the viability and power of these weapons.)

Goals and Challenges

Threat Assessment and Risk Management. Providing a thorough assessment of potential threats and an accurate, detailed model of the EPS that can be used for system design, attack scenarios (leading to policy and operational decisions), and simulations is the primary goal for threat and risk management. With the information from this assessment, risk management tools can be used to help management and system designers make well informed, rational decisions concerning policy and implementation of infrastructure systems.

The vast size and complexity of the system, coupled with the short response time available from real-time control subsystems provide significant challenges. The continuous evolution of technology and threats also poses a problem. With such a large and dynamic environment, model development and validation will be a continuous task.

Large Systems Analysis. An improved understanding of the intricacies and interrelationships among the many diverse subsystems that make up the electric power grid is the primary goal for the research effort for large systems. New models and simulations of the connectivity, logical and physical communication paths, and protocols of the overall system would embody this understanding.

Understanding and modeling such a large system are difficult tasks. Many communication mechanisms, protocols, and legacy systems are woven into the system. The verification and validation of the models pose another significant hurdle. As stated above, the continuous evolution of technology is a significant challenge and requires a long-term research effort.

High-security SCADA Systems. The primary goal of providing secure, hardened SCADA networks is to protect this critical link from internal and external attack.

Currently, most SCADA systems are protected by their obscurity and the need for domain-specific knowledge to pose a credible threat. An insider has the knowledge and expertise needed to mount an attack. The addition of encryption, authentication, authorization, and/or other measures to protect this critical link is a great challenge.

Changing the SCADA network would be disruptive and would require the interaction and support of a wide vendor community. Because standards-based solutions typically develop slowly, it would be difficult to migrate to a secure SCADA system within a timeframe sufficiently short to mitigate the risk of attack.

Efficient, Adaptable Encryption. A proposed new research area is in the field of adaptable encryption. The principal goal is to develop technologies that reduce the chance of compromising information transmitted over the EPS, without placing additional constraints or increasing the risks of lowering the performance of the existing communication network. Encryption systems that could respond to threats (e.g., dynamically increase security by using a stronger algorithm or longer key) and constraints (e.g., lower encryption overhead, switch to a decreased level of security, prevent cascade failure) would provide a powerful tool for designers of large distributed systems.

Encryption R&D would focus on methods to ensure signal security and fidelity without introducing latency or risk of signal degradation. Researchers would explore encryption techniques and the potential development of high-performance signal processing microprocessors that would handle encryption; evaluate protocols, particularly emerging protocols; and adopt methods to ensure signal security. Finally, they would collaborate with vendors for major software and hardware for SCADA, EMS, and control systems. Working with vendors would include conducting joint R&D efforts and performing field trials of new approaches for encryption for power system operations.

Robust Authentication and Authorization. Standardized, robust, and efficient authentication and authorization, which can be easily deployed to many applications, legacy systems, and communication protocols, are the primary goals of research in authentication and authorization. Developing, testing, and deploying such a flexible scheme are enormous challenges.

Intrusion Detection. Developing algorithms and other methods for detecting threats and attacks, even previously unknown attacks, while limiting the number of false alarms, is a daunting task. It is more difficult because of the size and complexity of the system, the numerous unique subsystems, and the short window of opportunity to mitigate a detected threat in the real-time environment.

Directed Energy Weapons. The goal of this research is to understand the threat posed by HERF weapons and then develop and implement preventive measures throughout the EPS. Difficulties in implementing such measures include the cost to design, build, and test such weapons in a reasonable environment. Also, it may not be feasible to implement preventive measures in some existing facilities.

Rationale for the Research and Desired Results

Threat Assessment and Risk Management. Currently, the information systems needed for large-scale EPSs do not have threat assessment and risk management tools. The lack of such tools makes it difficult to assess or manage an existing risk. With continuing deregulation and concentration of decision making, the risk continues to increase.

Large Systems Analysis. As the electric power industry becomes more and more interconnected, understanding these large, complex information systems is crucial for providing reasonable security. Without a solid understanding, even if research provides the necessary models and tools, the future growth of deregulation will continue to add vulnerabilities to this critical infrastructure.

High-security SCADA Systems. Currently, many SCADA networks on the grid are vulnerable to attacks from insiders and sophisticated adversaries. As deregulation continues and the use of shared communication channels increases, the risk of compromising SCADA networks increases. Research in this area is needed to mitigate the threat posed by the current trend of interweaving multiple, diverse systems over shared communication systems.

Efficient, Adaptable Encryption. Encryption can play a large part in mitigating vulnerabilities of the information infrastructure within the electric power industry. Encrypting information and control signals significantly increases the level of effort an adversary would expend in trying to obtain unauthorized knowledge of system behavior or seize control of power system operations (or portions thereof).

Robust Authentication and Authorization. Authentication and authorization schemes are effective measures for controlling risk in a high-threat environment. These measures are especially effective in regions where general access control is required, but they are also effective when multiple levels of security or authorization are required. Combined with encryption, the development and deployment of authentication and authorization measures for the power grid could substantially reduce some critical vulnerabilities.

Intrusion Detection. Detecting attacks is critical for providing a robust environment. This capability must be developed and enhanced to protect the power grid information infrastructure. It can be safely assumed that the power grid will continue to be a highly visible target and that probes and attacks will continue to increase. In this environment, intrusion detection, and the accompanying policy and procedure for mitigation, is crucial. Similarly, development of technologies and methodologies that enable appropriate and timely response to detected probes or intrusions is vital. Examples of response topics worthy of further research might include increased partitioning of the network and selective routing of traffic. Coordination among multiple parties collectively responsible for system operation creates additional challenges and research topics.

Basically, what is needed is to develop an appropriate, timely response, which clearly is a daunting challenge.

Directed Energy Weapons. As the availability of HERF weapons increases, their threat to the power grid increases. Because there is no known means for preventing a determined adversary from using these weapons, the risk must be mitigated through acquired knowledge (research), planning, development of mitigation technologies and preventive actions (implementation of mitigation technologies), and development of coordinated response plans.

Timeframe and Resource Requirements

Because the EPS is complex and our nation relies on it for our well being, the development and demonstration of systemic technologies are typically long and frequently expensive processes. The electric industry is the most capitalized in the nation, with equipment lives often measured in decades. Therefore, options must be developed so that information security technology and measures can be adopted to minimize risk.

Many of these activities are interdependent. Assessing threats and risks, understanding large systems, and developing secure SCADA systems are linked as base-level, architectural activities. Understanding large systems and developing credible threat and consequence models are a logical first step for evolving risk management procedures. Secure SCADA is an important part of the overall "large system." The numerous diverse systems, companies, and priorities will make the initial work in these areas difficult.

Developing, implementing, and deploying encryption will (most likely) be an evolving activity. It is difficult to retrofit encryption into legacy systems without introducing overhead and general system disruption. Because these conditions are not well tolerated in the power industry, the initial focus should be on developing robust, flexible and scalable encryption for deployment on new systems. Existing systems, which are both critical and vulnerable, should be identified and protected as soon as possible. This task implies a link to the projects on threat assessment and intrusion detection.

Research in encryption should be linked to the authentication and authorization project. Because portions of the authentication and authorization protocols will undoubtedly require encrypted channels, these activities should be carried out in parallel.

Research on intrusion detection should initially focus on deployed systems. A longer-term goal should be to engineer intrusion detection into the design of future deployments.

Research into high-energy weapons and their effect on this critical infrastructure should be tied closely to both the threat and risk assessment project and to persons concerned with physical security.

Table B.2 provides estimates of the timeframe and resource requirements for developing information assurance technologies for application in the electric power industry.

3.1.5 Emergency Response and Recovery Information Technologies

Description

Electric power grids in the United States rely heavily on a complex, interconnected network control system and are expected to do so in the foreseeable future. This system is widely dispersed and highly vulnerable to computer-based intrusions and attacks. Effective ways to identify, respond to, and recover from attacks on the information systems that underpin this interconnected network are not well understood. Utilities are experienced in responding to and recovering from disruptions in their physical system, such as those caused by hurricanes, floods, and other natural disasters. Developing emergency response and recovery protocols and procedures for information technology systems within electric power grids is an area requiring future R&D.

This effort would involve both basic and applied research. One way to institute emergency preparedness from a national security point of view would involve the concept of a minimum essential information infrastructure (MEII). The MEII concept would identify the minimum portion of the electric power grid information infrastructure necessary to ensure the grid's continued functioning even in the face of a sophisticated strategic cyber attack.

Table B.2 Estimates of Timeframe and Cost for Information Assurance and Cyber Security

Topical Area	Timeframe (yr)	Cost[a]
Threat Assessment and Risk Management	3–5	25
Large Systems Analysis	5–10	45
High-security SCADA Systems	5–10	80
Efficient, Adaptable Encryption	3–10	75
Robust Authentication and Authorization	3–10	75
Intrusion Detection	3–10	75
Directed Energy Weapons	3–10	60

[a] Costs are estimated in millions of U.S. dollars.

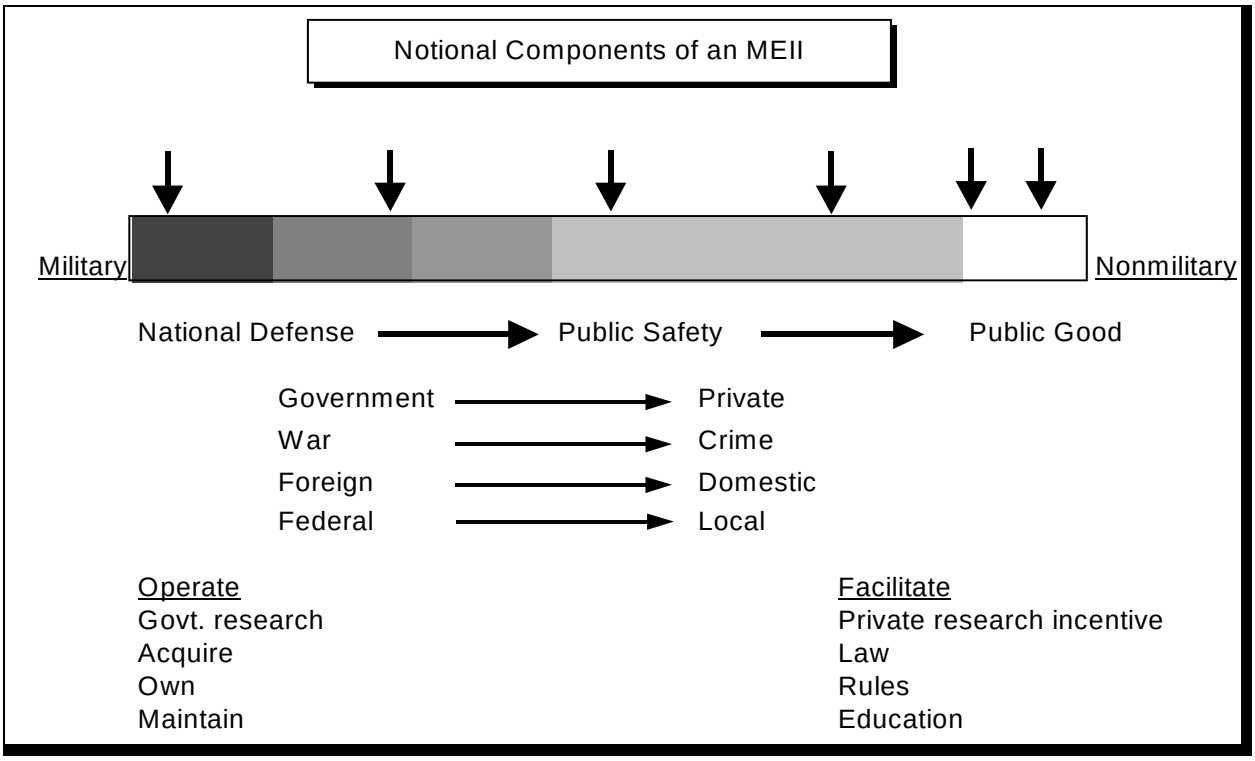

Figure B.2 Spectrum of National Security Preparedness and Government Roles for the Electric Power System Infrastructure (adapted from Molander et al. 1996)

Figure B.2 shows the spectrum of different kinds of preparedness across the electric grid information infrastructure.[5] The traditional military preparedness (left) and the nonmilitary (right) means of preparedness are shown. Moving from left to right the events resembling war tend to look more like crime; foreign threats look more like domestic threats; government responsibilities move to private issues; and within government, the level changes from federal to local.

It is not feasible to protect the entire electric grid information infrastructure from attack. In Figure B.2, the vertical arrows along the top of the spectrum represent "point defenses," defined by selecting those parts of the infrastructure most critical to military and civilian operations and then defending them in appropriate and affordable ways. For example, an arrow on the far left could indicate a portion of the grid information infrastructure critical to military operations that would be placed on dedicated fiber-optic cables. An arrow on the far right could be a tax incentive that would encourage utilities to cooperate with U.S. government-led protection processes and to develop reconstitution capabilities. Point defenses between the far left and far right can be implemented by some combination of laws, regulations, and tax incentives.

[5] Molander, et al., 1996, *Strategic Information Warfare: A New Face of Warfare*, RAND MR-661-OSD. This document is available at (http://www.rand.org/publications/MR/MR661/MR661.pdf).

An exercise methodology could be used to analyze the problems in identifying, responding to, and recovering from cyber attacks on the electric power grid. Participants in the exercise would be presented with hypothetical future crises and asked to develop appropriate responses. Responses would address issues that occur during and after the crisis. Shortcomings and weaknesses in the response would be identified and ways to correct them proposed.

The initial product of this research would identify the minimal essential components of the information infrastructure that are critical to the continued functioning or reconstitution of the electrical grid. Another product of this research would be development and implementation of a set of rules, regulations, and tax incentives, sponsored by the federal government, that would encourage owners and operators of the electric grid to reduce their infrastructure's vulnerability and/or ensure rapid recovery from an attack.

Another product may be developing computer simulation models that utilities can use as training tools for conducting MEII emergency response exercises for utility system personnel. Periodic exercises would help ensure that utility personnel are familiar with their MEII emergency response plans. Exercises can also be used to fine-tune the plan as changes occur in the electric power grid and in information technologies. This approach is similar to using utility control room simulation to train operators on routine and emergency operations of the grid (as opposed to the information system).

Another product could be designation of a "red team" chartered to conduct and evaluate attack exercises on hardware and software. Benefits would include increased realism, focus, and urgency for the program at large; reality checks on priorities; feedback that would help decision makers adjust research milestones; additional stakeholders; and increased potential support.

Goals and Challenges

Achieving some of the goals and challenges of this research may be especially difficult. Given the diversity and subtlety of attacks within the information infrastructure, it will be necessary to detect and differentiate among mistake, accident, deployment of software agents designed for espionage, and predeployment of software weapons. Even after the essential elements of the electric grid's information infrastructure have been identified, it may be necessary to develop technologies to protect them.

The fact that the private sector controls or owns major portions of the electric power grid may present a significant challenge. However, studies can be conducted to determine an optimal combination of government policies, procedures, regulations, and tax incentives needed to encourage owners and operators of the grid to reduce vulnerability and ensure rapid recovery from cyber attacks. The private nature of the business, combined with the public image requirements in a competitive environment, often keeps utilities from disclosing attacks, particularly successful ones.

To ensure that owners and operators of the grid maintain a high level of preparedness, it will be necessary to develop a program to exercise electric system personnel on a periodic basis. Exercises would test coordination between the public and private sectors. Computer simulation models could be developed and used as training tools to conduct exercises for utility system operators. The capability to share and implement lessons learned during the exercises should also be developed.

Additional challenges to the research could arise from deregulation of the electric utility sector. Competing companies may be reluctant to share critical, essential, or sensitive information. Procedures will need to be developed so that utilities do not compromise their competitive positions by cooperating in certain activities.

Finally, perception of excessive government interference needs to be addressed. The government's role in national security preparedness must be balanced against public perceptions of the loss of civil liberties and the commercial sector's concern about unwarranted limits on its practices and markets.

Rationale for the Research and Desired Results

This research is important because it could help mitigate an urgent infrastructure threat/vulnerability. Because it is not possible to completely eliminate a vulnerability, it is necessary to develop contingency plans to minimize the effects of an attack or disruption. Procedures and protocols for identifying, responding to, and recovering from cyber threats to the electric grid are areas that have not received enough attention. The interconnected nature of the grid and the impending transfer of large blocks of power over several grids makes it more important than ever to ensure that utilities coordinate their efforts in emergency response and recovery. Therefore, the risks of not having this framework available in the timeframe of interest are potentially significant.

Timeframe and Resource Requirements

In the near term (i.e., before 2000), the MEII concept could be developed. Critical components in the information infrastructure of electric grids could be identified and ways to protect them explored. Protocols and policies to implement the concept, as well as computer simulation models to use in the exercise process, need to be developed. By 2005, exercises would be conducted on a periodic basis and the process refined as necessary. A capability to share and implement lessons learned from the exercises would be developed and applied. By 2010, the exercise process would be fully mature. However, as changes occur in the structure of the electric grid and in information technologies, the process would be refined to address those changes. The estimated level of resources required to develop and implement the MEII concept to full maturity is about $10 million.

This research is not limited to the electric sector. Oil and gas pipelines are highly interconnected networks and also vulnerable to attacks on their imbedded information infrastructure. Consequently, this research area is very applicable to these networks.

Depending on the experience with implementing the MEII concept in the electric sector, development of the concept for the oil and gas pipeline network could begin after 2000.

3.1.6 Transmission and Distribution Technologies

Description

The transmission and distribution (T&D) components of the electric infrastructure deliver power to meet customer loads. The integrated network is frequently divided into high- (greater than 100 kV) and low-voltage (less than 100 kV) systems. Increasing the capacity and capability of existing T&D systems improves system reliability by increasing margins to system thermal and stability limits. Technologies that relieve congestion will improve reliability under the demanding conditions of a competitive power market.

The construction of new power lines to expand transmission capacity has slowed in recent years by more than one-third, in part because of public concerns about the aesthetics of transmission towers and lingering concerns over the health risks of electromagnetic field exposure. Because of the difficulty in finding acceptable sites for new transmission lines, utilities are looking for ways to increase capacity. One way is to increase the rating of existing lines or add (repack) lines in existing corridors.

Flexible AC Transmission System (FACTS) technologies now being developed and tested are replacing electromechanical controllers, which are too slow to govern the flow of current in real time, resulting in loop flows and bottlenecks. FACTS controllers can increase or decrease power flow on particular lines to alleviate system congestion. In addition, FACTS controllers can enhance system reliability by counteracting transient disturbances almost instantly by allowing lines to be loaded closer to their thermal limits. Two generations of FACTS controllers are currently in service, and a third generation is nearing demonstration. Further R&D is required to adapt these devices to specific uses and to reduce their costs to practical levels before they can be adopted nationwide. FACTS technology will eventually be deployed nationwide, because it is an essential component in a true open power market with acceptable levels of reliability. Accelerated support could cut the costs of FACTS devices by one-quarter and speed their deployment.

Recent studies suggest that with the new FACTS technologies, remote interactions that involve controls in one end of the system can, at times, have a profound effect on distant regions of the system. Clearly, these concerns need further analysis because the threat is twofold:

- It is possible to have adversely affect the grid from long distances.
- Any need for coordinated control over long distances without means for backup control if the system is disrupted is likely to be counterproductive during emergency conditions.

Wide bandgap semiconductors (WBSs) — primarily nonsilicon materials such as diamond thin films, Group III nitrides, and silicon carbide — have the potential to dramatically reduce the cost of power electronics controls for the intelligent network. The WBS could result in an "integrated circuit of power electronics" by replacing complex, multi-thyristor switching devices with a single, multifunction controller. Ultimately, WBSs could greatly reduce the costs of FACTS and custom power systems and speed their deployment.

With further development, the WBS has potential for lower cost, greater reliability, higher current density, and reduced size. The nation that leads in WBS commercialization will gain a major advantage worldwide. Currently, American manufacturers significantly lag behind their Japanese and European competitors. Forming a nationwide consortium could substantially speed U.S. development of this technology, which would allow the United States to become more competitive.

Hierarchical control of FACTS, which requires more highly integrated, centrally coordinated control by system operators, is needed to integrate the actions of multiple FACTS devices as they come into widespread use. This hierarchical control will raise the power transfer limits of transmission systems over wider areas, eventually extending from coast to coast. Utilities and power pools also need the capability to understand disturbances that develop in neighboring regions to ensure that they do not spread and that stability is maintained throughout the continental grid.

Implementing hierarchical control requires real-time communications and monitoring capabilities, as well as on-line system analysis. Although work has begun on these capabilities, their completion and implementation throughout the North American grid is expected to take at least two decades of intensive effort.

Underground T&D cable systems are a vital part of many networks, and utilities are increasingly using these systems to deal with problematic overhead lines. Underground transmission provides an alternative in large population centers. It has supplied critical downtown loads in large cities for decades, and now is increasingly being used in suburban and rural areas. However, underground transmission has historically been a costly alternative—ranging from 2 to 20 times the cost of an overhead line, depending on operating voltage and installation environment. In addition, the industry is moving toward cables with cross-linked polyethylene (XLPE) insulation to avoid the environmental risk of leakage of the dielectric fluids used in traditional cable systems. Concerns about the reliability of the XLPE systems at higher voltages abound.

There is a need to develop direct-current (DC) transmission; the biggest hurdle to this development is AC/DC converters. Also, vendors are primarily located in Europe.

Many existing underground transmission systems are aging, leading to concerns about reliability and the cost of maintaining system performance. Load growth in urban centers, where most of the underground transmission systems are installed, is increasing at a rate of 4% to 5% per year. Installing new systems is difficult and costly, and

reliability requirements are increasing. In this environment, utilities and system operators need a way to increase the capacity of existing circuits while improving reliability and service life. Research is needed to find ways to reduce the costs of new systems, increase the public's confidence in high-voltage XLPE cable systems, and maximize the use of installed cables.

Custom power involves the use of solid-state power electronics to control distribution systems. While the technology is essentially the same as FACTS, the scale and complexity of the installations are smaller. Within 10–20 years, custom power controllers should provide the interfaces needed for widespread use of distributed generation. These interfaces would perform four critical functions:

- Control the bi-directional flow of power between the distribution network and small generators on the customer's property.
- Provide voltage conditioning to the output of a small generator before it enters the network.
- Correct network stability problems that might arise from the presence of many distributed resources.
- Provide on-site reliability and enhance power quality.

Custom power devices also will be used in distribution automation applications to provide real-time network control and reduce system operating costs. Their use must be researched carefully to characterize system behavior during emergencies.

The first custom power devices are beginning to enter utility service, approximately 5–10 years behind FACTS. They are expected to become commonplace as the price of electronic components continues to decline. The major problem is cost; more intensive R&D is required to achieve the substantial savings needed in a competitive timeframe. This R&D would focus on re-engineering custom power devices for greater efficiency and developing better device control methods. WBS technology, as noted above, could also be applied to custom power applications with appropriate research.

High-temperature superconductors (HTSCs) have developed rapidly (only 10 years from discovery to prototype applications), implying that these devices could profoundly affect the electric power industry over the next two decades. One area of high potential impact is the use of HTSCs in the power delivery infrastructure to meet growing customer demand for more power at higher levels of reliability and lower costs.

An individual HTSC wire can carry as much as 100 times the current of an ordinary conductor, and HTSC cables promise to offer at least double the capacity of existing underground conduits for a given diameter and voltage. They could therefore provide an important upgrade option for satisfying demand growth on heavily loaded distribution systems, while making underground transmission a more economical

alternative to overhead lines — reducing electricity rates to consumers by transferring low-cost power over longer distances.

The HTSC cables for distribution systems are expected to be particularly attractive for retrofits in the crowded urban underground network. The increased capacity resulting from using existing duct banks would permit major new commercial and industrial developments to be added, while minimizing the disruption (e.g., tearing up city streets and re-routing traffic). However, unless the mean time between failures is very high, having more customers (load) per distribution circuit may reduce reliability.

High-voltage transformers made with HTSC materials can be designed so that they are one-half the weight of conventional units and have a smaller footprint. In addition, HTSC transformers can reduce power losses and operate more efficiently than their conventional counterparts.

Application of superconductors to equipment such as transformers adds efficiency, but also drastically different characteristics. Integrating this equipment with conventional types may lead to many new problems.

New methods of stationary energy storage are on the horizon. They have the potential to level the hourly demand of power plant facilities and provide new ways to increase the reliability of power delivery. Environmentally sustainable hydrogen production (from solar, wind, and nuclear sources) is the most dramatic possibility, for use both in fuel cells and in direct clean combustion. Other promising future storage options include large-scale ultracapacitors, advanced flywheel systems, and superconducting magnets.

Rapid-response energy storage can greatly expand the effectiveness of custom power devices needed for improving retail service. One candidate is the superconducting magnetic energy storage (SMES) system. A project to build a 20-MW SMES capable of providing ride-through for outages of a few seconds using current technology would cost approximately $30 million. Further development of HTSCs may eventually change this picture because HTSCs require much less expensive refrigeration. However, HTSC technology is not yet ready for SMES use. Continued HTSC development, particularly in superconducting materials development and wire fabrication, is crucial to long-term practical SMES use, as it is to other valuable future technologies, such as large generators and motors, power transmission lines, and magnetically levitated high-speed transportation.

Flywheel energy storage (FES) devices also show good potential because they are highly efficient, transportable, operationally robust, and require relatively little maintenance. Small FES devices using superconducting bearings have been developed at the laboratory scale. Larger, higher-performance, more economical, and field-tested devices are needed.

Ultracapacitors of the near future may increase energy storage capacity of conventional capacitors by millions. In addition, ultracapacitors can release their energy 10 to 100 times faster than batteries. Applications may include hybrid electric transportation, power quality and outage ride-through assurance, manufacture of advanced materials, and communication devices. Specific research is needed in miniaturization, large-scale manufacturing methods, and cost reduction.

Goals and Challenges

The challenges for improving the T&D systems fall into three broad categories: materials, devices, and systems. Materials advancements are at the core of two critical enabling technologies — HTSC and high-power electronics.

Superconducting cables have been fabricated in 300-m lengths, but additional improvements in fabrication processes are needed to achieve lengths in the range of several kilometers, which is both a reasonable increase in scale from present capability and a useful length for commercial application in utility distribution systems. Significantly, the near-term challenge for HTSC is not to increase the transition temperature, but to reduce the cost of fabrication and to improve the performance of cryogenic systems and thermal insulation at less cost.

Advanced semiconductors for power electronic devices facilitate fast control of power flows at lower costs so that the technology can actually be deployed. Fast control increases reliability by increasing the steady-state transfer capacity of the system; flows are routed on lines with available capacity. Fast control allows the system to respond rapidly enough to maintain stability under contingencies conditions.

Other goals and challenges include:

- Reduced cost and improved reliability for instrumentation and control;
- Proof of principle and validation of the reliability of large, “smart” systems;
- Siting and environmental impacts of new transmission capacity;
- Large-scale simulation to assure that the complex distribution system is reliable;
- Hardening the T&D system against sabotage and physical threats; and
- Long-term reliability of thermal insulation.

Rationale for the Research and Desired Results

Improvements in T&D equipment affect all aspects of power system planning and operations and indirectly improve system security and reliability. Increased transmission margins significantly lessen the likelihood of reaching critical system limitations, thereby

avoiding cascading system outages. Additional operating flexibility helps systems to recover from disturbances. Larger operating margins provide system operators with alternative methods for resolving emergency conditions, thus increasing system reliability.

Advances in HTSCs and semiconductors for power electronics will contribute to advances in T&D components and system design. Measures that will maximize the use of existing transmission corridors, through either compact tower designs, or underground transmission, will lead to more secure system operation.

Rapid-response storage devices at suitable locations can mitigate the effects of severe events by providing emergency power and preventing cascading outages.

Timeframe and Resource Requirements

This topic involves many potential R&D projects and demonstration facilities (e.g., 20-MW SMES at an estimated cost of $30 million). Substantial progress is needed in each of the several research areas listed above. Although industry contributes substantial funds to the general area of T&D technologies (e.g., FES), there is an important federal role in pursuing R&D that is especially relevant for infrastructure assurance (e.g., SMES) and longer-term, high-risk R&D. The R&D funding needed through 2010 is more than $500 million.

3.1.7 On-line Security Assessment

Description

Electric power system operators need to operate the system safely within allowable tolerances on line loadings, voltage levels, and frequency under varying conditions. Computations that attempt to assess whether the operating system is safe are called “security assessments.” On-line security assessments use near real-time data to predict system performance under assumed or anticipated system disturbances and identify preventive measures to maintain the system in a safe operating state. OSAs can also be used in system restoration planning.

Utilities must be able to conduct OSAs so that they can cope effectively with power system contingencies, especially multiple simultaneous faults. OSAs include power flow (feasibility) computations over many contingencies, optimal power flow-based redispatch, and on-line transient analysis.

The following components are needed to perform an OSA:

- *Accurate models of the system*. The August 1996 western outage revealed that system models had not been adequately calibrated or tested for the unusual circumstances and event sequence that led to the outage. Model calibration is expensive and needs to be improved. Research on network “equivalencing” is also needed.

- *On-line analytical tools*. On-line analysis is in its infancy. The first generation of software can now provide operators with near real-time information on system conditions. Analytical tools are needed to reduce the time required for analysis and recommendations.

- *Accurate, timely, synchronized information on the system state.* In many areas of the country, information about the state of the system is not readily available from remote sites. Although the Wide Area Measurement System (WAMS) shows promise in remedying this problem, very accurate synchronization of state information (within a fraction of a cycle) is needed to identify incipient stability problems. Timing signals from Global Positioning System (GPS) satellites can be used to provide this synchronization.

- *Communication system to collect, store, and transmit system state data*. Advances in the rate of data collection from a geographically dispersed sensor network are needed as a prerequisite to detailed real-time calculations.

- *Real-time database systems.* Current systems are difficult to modify because of ad-hoc, proprietary designs. The system should include telemetry data, state estimates, and computation results.

- *State estimation software*. Improved state estimation software is needed to resolve differences among measurements and to predict future states. Distributed and parallel computation methods are needed to exploit major technologies for building high-performance computational systems.

- *Algorithms and facilities for performing the security assessment computations.* Perhaps the most difficult challenge in implementing OSA is the development of improved algorithms for accurate, timely calculations. Fault scenario screening tools, parallel or distributed computing facilities, improved algorithms for solving large sparse matrices, and incremental algorithms that do not require recomputation for added faults are candidates for research initiatives.

- *Integrated security assessment system*. The security assessment system must be highly reliable and immune to faults. Issues relating to the security of the system involve trade-offs between a large centralized facility (housing all data and processing systems) and distributed computing and data storage facilities. Various options need to be evaluated, including cost/benefit studies. Probabilistic risk assessment tools should prove valuable in these evaluations.

Goals and Challenges

On-line security analysis systems need substantial improvements in performance to meet the functional requirements for preventing and reducing the effect of power grid disturbances. Current systems require about 15 minutes (approximately 1,000 seconds) to analyze a complex power grid. However, detecting system faults and taking corrective

action require state calculations every few cycles, 10,000 times faster than current capabilities. Another requirement calls for processing orders of magnitude more input data, which implies extremely large improvements in processor speed and probably massively parallel and/or distributed architectures. It may be advisable to investigate probabilistic and agent-based computational methods for analyzing large systems, rather than rely on the traditional deterministic approach.

A second challenge relates to input data requirements. Most transmission and distribution systems have rudimentary instrumentation systems, often based on analog sensors, characterized by low data rates, and infrequently calibrated. OSA requires digital sensors, data buses, and "smart" sensors capable of self-calibration and fault diagnosis. Instrumentation and control systems developed for other industries can be adapted to the needs of the power grid, but the power industry faces a significant challenge because of the sheer numbers of geographically dispersed sensors required.

Rationale for the Research and Desired Results

OSA will be most useful in preventing or mitigating damage from cascading faults. The 1996 western outages were caused by cascading faults. A single fault created a disturbance that propagated through a large system, which ultimately resulted in an outage that affected millions. If a suitable OSA system fed by detailed power grid data had been in place at the time of the initial disturbance, the cascading outage probably would have been prevented and damage would have been limited to the vicinity of the initiating event.

Developing suitable OSA systems also will allow analysis of the signature of various system disturbances. For example, it should be possible to differentiate natural or accidental initiating events (e.g., overloads during peak demand periods, transmission bottlenecks, system instabilities) from deliberate acts (actuating breakers at substations, shooting at transmission lines).

However, current OSA systems are not capable of monitoring, controlling, and simulating large power grid systems. Sensors and communications systems need to be developed for handling large parallel data streams. Algorithms for analyzing these data and for recommending changes to the operation of the system also need to be developed to prevent or mitigate disturbances.

One alternative to using algorithms may be coordinated dispersed controls. Substantial R&D is required, but this approach could reduce data communication requirements.

In the near future, the reliability of the grid also will be tested by the increasing demands for access to transmission resources in an open power market. The demand for transmission resources will affect the grid, but it is difficult to predict in what ways. However, the operating state of the system may be somewhat different than it is now. OSA will be useful in predicting stress on the grid caused by the open power market.

Furthermore, advance information on upcoming transactions and demands for transmission resources will provide useful input for the OSA. The OSA can use these data for computing system stability and thus help grid operators anticipate future demands on the system. This "look-ahead" capability implies additional enhancements of OSA algorithms to analyze both short- and long-term time dependencies.

Timeframe and Resource Requirements

In the next few years, a 1,000-fold increase in speed with subcycle state information can be achieved. By 2005, accurate models and tools for the national grid can be devised. By 2010, new tools and techniques for OSA will be developed. Funding requirements through 2010 are estimated to be $50 million.

3.1.8 Dispersed Generation and Backup Infrastructures

Description

Renewable-resource Generation. Advanced renewable electric energy sources (solar, wind, hydro, and biomass) have the potential for significantly increasing the diversity and flexibility of electric generation, conserving fuel resources that reduce the carbon intensity of generating electricity, and reducing dependence on a single-source fuel supply. The advantages of this diversity are increased competition among generation alternatives, resulting in cost savings for electric energy and a greater degree of choice for the consumer. This flexibility will make the overall system more resilient and able to cope with naturally occurring disruptions.

As concerns mount about urban pollution and global warming, these renewable technologies grow more attractive. Both solar and wind technologies are now at an economic disadvantage for generating bulk power compared with fossil fuel. Moreover, the current wholesale power market in the United States is characterized by very low marginal prices and a glut of fossil and nuclear generation, which does not favor the introduction of new generation resources. In the next decade, the market must adjust for decommissioning of nuclear plants and retirement of old coal-burning plants. Renewable generation in developing countries, however, may be more attractive in the near term and could become a major export opportunity.

Renewable resources are sustainable because their availability is unlimited, at least from a global perspective, in quantity or time, and because they have little effect on the planet's ecosystems. Renewables are also suitable for distributed generation. Thus, they offer the potential for making the power system more resilient and reliable by locating electricity generation near the point of use. However, renewables will not become more than a niche generation alternative without technical advances to improve performance and reduce costs.

Solar Photovoltaic Power. Steady improvements in the technology of converting sunlight directly into electricity have led to the production of viable "off-grid"

power systems. With a small solar system in place, a remote village in a developing nation could have refrigeration, communication, a light source, and some pumping capability.

Currently, these systems have far-reaching applications in the developed world. Cellular telephone installations, signal repeater stations, water pumps, isolated homes, and weather stations in remote locations are routinely powered by solar energy systems. More than 100 MW of solar electric installations operate worldwide. The solar electric industry is on the verge of mass production of portable power generation units suitable for installation as self-sustaining, affordable electric supply systems in developing nations or in remote locations in the United States.

The technology of solar electric conversion must improve substantially before it becomes an economically viable alternative to grid power in developed countries. The conversion rate from solar energy to electricity is about 7% new. Research indicates that the conversion rate could double or triple within the next few years.

For example, with flat-plate photovoltaic solar energy conversion technology, an energy conversion efficiency of 15% is possible for direct or indirect sunlight. Overall life-cycle delivered electricity costs are competitive with fossil and nuclear central station power. However, several key knowledge gaps exist. Additional development is needed for triple-layer photovoltaic cell materials and manufacturing processes. Long-term stability at 15% efficiency needs to be assured to meet cost targets. For amorphous silicon photovoltaic technology, a competing approach, costs are potentially very low, but additional development of manufacturing processes is required.

Wind Power. Wind energy is available in many locations worldwide. The newest, most technologically advanced wind installations can produce power at rates comparable to new fossil generation. However, new wind power installations in the United States must compete with existing fossil, nuclear, or hydro power plants, which produce energy at extremely low prices.

Given the nature of today's wholesale U.S. electric power market, which is characterized by very low marginal prices and a glut of fossil and nuclear generation, the construction of large new wind power stations in the United States in the near future seems only a remote possibility unless driven by carbon-reduction needs. "Green" pricing and renewable portfolio standards offer potential for expansion of wind power and other renewables. Wind installations in developing countries, however, may be more attractive and could become a major export opportunity as well as an environmental gain.

Biomass. Burning plant matter (wood chips, sugar cane bagasse [remains of sugar cane after the milling process]) has contributed to electricity production for many years. Biomass combustion reduces emissions compared with coal-fired plants and essentially emits no CO_2. Research into biomass electricity production in the United States currently is small and focuses on co-firing biomass fuels with coal in conventional power plants and on growing genetically engineered crops that could be used as fuel for

power plants or for other products (fiber, food). Additional research is needed to develop better systems for biomass combustion and to explore gasification and other applications for the use of biomass.

Distributed Generation. Distributed generation technologies, including fuel cells, photovoltaics, microturbines, diesel engines, and energy storage devices can provide another path for diversifying electricity generation. Distributed generation also increases flexibility for users of energy. They can insulate themselves from grid reliability problems; use gas and electricity interchangeably, depending on the relative prices of gas and grid-supplied electricity; improve efficiency; and reduce costs. Depending on the technology, distributed generation systems can operate on such diverse fuels as biogas, methanol, and hydrogen.

Fuel cells are a key technology for achieving fuel diversity, particularly in distributed generation. Investigations range from fundamental research on materials to increasing unit efficiency to field demonstrations of early units. Phosphoric acid fuel cells are already commercialized and operating at 75 sites worldwide, achieving efficiencies of 35% to 45% and an overall availability of 95%. Continued development is addressing technical, operating, and economic issues to make this option cost-effective. Commercial molten carbonate fuel cells — which can accommodate such unconventional fuels as landfill gas, digester gas, and biomass fuels — should be commercially available by 2002, as work in progress addresses technical issues and reduces balance-of-plant costs. Other promising fuel cell technologies — solid-oxide fuel cells and polymer electrolyte membrane fuel cells — are also being pursued.

Goals and Challenges

Large-scale integration and simulation are needed for distributed generation systems. There is a need to understand how to control a large number of dynamically interacting distributed resources. Also, integration is needed for massive numbers of instrumentation and control systems.

Researchers need to find methods to reduce costs and improve reliability of small-scale power generation systems. Another important challenge is the ability for the systems to run unattended for long periods of time.

For advanced backup power systems, improved control systems applied to existing backup generators are needed. Also needed are policy changes to allow backup systems to power the distribution system in emergencies.

Rationale for the Research and Desired Results

The improved diversity and flexibility of electrical generation are major benefits of renewable sources; there also are benefits to infrastructure assurance. The environmental and sustainability benefits are likely to be even more important in the

coming years. Finally, distributed generation can reduce the likelihood of regional blackouts from large-scale grid problems.

Timeframe and Resource Requirements

This topic has a number of worthy R&D areas at different levels of development. The electrical industry and the federal government are investing substantial funds in related R&D. Federal support that emphasizes the infrastructure assurance aspects of these research areas is needed. Estimated additional funding needed through 2010 is $100 million.

Improved energy storage devices (rapid response systems were described in Section 3.1.6, Transmission and Distribution Technologies) could also contribute to system reliability through distributed siting. Options include flywheels, batteries, and superconducting systems.

3.2 Oil and Natural Gas Systems

3.2.1 Critical Consequence Analysis

Description

The U.S. natural gas pipeline transmission network is the interconnected sum of a large number of privately owned and operated gas pipeline networks. While each pipeline company has full knowledge of its assets and the operations of its own network (intakes, deliveries, flows on pipeline links), no one — private company or governmental agency — has a clear, detailed picture of the operations of the whole system, nor does any outside company know how the various subnetworks feed into each other and are balanced over time. Because of this interconnectedness, disruptions in the physical system of one company may have far-reaching consequences, such as a lasting interruption of gas supply to a major metropolitan area or a major electric power generating plant, or no consequences at all because the structure and capacity of the overall network frequently allow for alternate gas supplies to be easily rerouted to these consumption nodes. Developing a thorough understanding of the possible consequences of physical failures, as well as strategies for optimally coping with them, is in need of future R&D.

This effort involves elements of basic research (mathematical modeling of complex networks) and applied research (data analysis and model computer implementation). The proposed research centers on the development, calibration, and computer implementation of gas network simulation and/or optimization models. Researchers would develop a detailed network representation of the U.S. system, including all interstate and intrastate pipelines, to the distribution city gates and beyond. Each delivery point could be characterized by a curtailment impact index — the higher the index, the more catastrophic the impact of one unit of curtailment.

These models would be used ideally to test the vulnerability of the network under different incident scenarios (one or several links, compressors, storage fields, or interconnections are out of service). The source of the incident can be either a physical or cyber action. The model would then attempt to reroute the available gas while minimizing the total impact of the curtailment. If rerouting is successful and the total impact is nil, the nodes/links assumed to be inoperative can be considered noncritical. Alternatively, if deliveries to a major metropolitan area must be curtailed, the nodes/links are critical and should be given a high priority in any risk management approach. The models could be used to test numerous incident scenarios, from which researchers could derive an ordered list of critical system components (links, compressors, storage fields, interconnections).

The products of this research include (1) information on critical network components and on the consequences of their failure; (2) a system of computerized models (software) that could be implemented on powerful PCs, workstations, or mainframes; and (3) a set of rules or procedures for mitigating the negative effects of incidents once they have occurred.

Goals and Challenges

The overall goals of this project are to identify critical components in the U.S. gas transmission network, assess the consequences of any dysfunctions, and propose strategies for mitigation. These goals would be achieved with the help of computerized models. A fundamental difficulty in this research is to design sufficiently detailed models that provide useful answers to various questions, while remaining manageable from a computational and data input viewpoint. The size of these models may prove to be a serious challenge. Simplifications (e.g., network aggregation) may be necessary, but they would have to be tested carefully so that they do not decrease the overall usefulness of the models. To build the models, publicly available information at the federal level (FERC, DOE, DOE's Energy Information Administration [EIA], U.S. Department of Transportation [DOT]) would have to be complemented by data from state governments (e.g., public utility commissions) and by data from pipeline companies, particularly intrastate pipelines, and major local distribution companies. These companies may be reluctant to share the necessary data (e.g., gas flows) because of competitive pressures; appropriate procedures would have to be developed to protect these data while establishing cooperation with these companies.

Rationale for the Research and Desired Results

This research is important for the following reasons:

- A network representation of the U.S. gas system is the only way to understand, in an operational fashion, how the system works.
- Models are essential for vulnerability assessment, particularly for identifying and ranking the weak components of the system and determining where risk management resources should be allocated.

- Models can be natural tools for mitigating the negative effects of incidents and for planning recovery activities (e.g., prioritizing recovery actions).

- Models would also allow for interfacing with the natural gas infrastructure and the power infrastructure, particularly at the level of gas-consuming power plants.

Timeframe and Resource Requirements

This R&D project is classified as most important. The issues involved are physical threats, complexity, and interdependencies. The time needed to complete the project is about four years. Resources of $3 million are needed.

Three major activities have been identified for "Critical Consequences Analysis" that would span the four-year duration of the project:

- *Basic model design.* This activity would be completed in Year 1. The mathematical structure of the model(s) would be designed, and decisions would be made regarding the level of model detail or aggregation and the type of necessary input data.

- *Model development and implementation.* This activity would be completed during Years 2 and 3. Activities would include processing and analyzing the input data obtained from public and private sources, programming the model, debugging it, and testing it to ensure that it is a reliable representation of the U.S. gas transmission network. This testing may lead to model adjustments.

- *Consequence analyses.* This activity would be completed in Year 4. Numerous incident/failure scenarios would be developed and input into the model(s). The model(s) would be run and the resulting curtailment impacts analyzed. This analysis would lead to the development of an ordered list of critical network components (e.g., supply sources, storage fields, compressors, pipeline links, and interconnections).

3.2.2 Decision Support Systems

Description

This purpose of this research is to develop and implement risk management and decision support tools to allow gas and oil industry decision makers to prioritize resources, thus minimizing risk and effectively responding to incidents.

Predictive Risk Management. Mitigation of risks to both processing (e.g., gas processing plants or oil refineries) and piping systems is an important element of private-sector management of such physical facilities. As a result, gas and oil production, transportation, and delivery are relatively low-risk activities. Nonetheless, past pipeline failures caused by third-party damage or mechanical failure have been costly, and industry activity in risk management is increasing. Furthermore, the increasing system

complexity and interdependencies, described elsewhere in this report, exacerbate the potential impacts of incidents. These changes occur at a time when energy industry deregulation calls for overall reductions in production and delivery costs.

Response and Reporting Decision Analysis. Following recent oil and gas pipeline ruptures, the industry joined with the federal government to improve risk management tools. DOT is currently funding a demonstration to determine the safety and economic advantages of risk management processes. Despite this important progress, the development of risk management tools and decision support models is in its infancy. Use of decision models (e.g., Pipeview™ or Pipeline Maintenance Optimization System) is very limited. Spatial analysis tools, such as the Integrated Spatial Analysis Techniques, funded by the Gas Research Institute, are under development. However, these systems focus entirely on the physical risks to the oil and gas pipeline industries. These technologies need to be developed and applied both upstream to production and downstream to distribution and expanded to include both cyber and physical threats.

Incident reporting and response are other areas of increasing concern to industry and government decision makers. The gas and oil industry currently uses sophisticated procedures for emergency response. However, the increasing complexities and interdependencies in the evolving energy business also illustrate the need for development of decision analysis tools.

Another important consideration in the development of decision analysis tools for prediction, mitigation, response, and reporting is the continuing development and application of new sensors for monitoring and inspection. As these technologies (Section 3.2.4) evolve, decision analysis tools need to be continually upgraded to take advantage of improvements in data input.

Goals and Challenges

Predictive Risk Management. Risk management models are needed that allow integration of real-time operational control data (e.g., processing plant/refinery process controls, pipeline SCADA) with detailed physical history data (e.g., construction type, past inspection information, maps, component types, repair history, environmental history). These models are needed for each sector of the industry — production, processing, transportation, storage, and distribution. Development of an enterprise-wide model requires careful consideration after sector models have proved to be effective.

The overall goal of risk management is to increase security and safety while minimizing operating costs. Specific goals for predictive risk management models include the following:

- Provide a comprehensive description of the physical and cyber properties of the industry segment using spatial (e.g., geographical information system, GPS) methods.

- Incorporate an interpretive capability, including historical operational, inspection, data transfer, and electronic commerce information in decision analysis.

- Include a predictive capability to allow optimized resource allocation to maintenance, repair, inspection, capital improvement, or computer system/software upgrade activities.

- Provide real-time recognition of high-risk conditions (physical or cyber) caused by natural system deterioration (e.g., corrosion, cracks, sensor failure), operator error (or intentional action), or third-party intrusion.

- Incorporate an element to resist tampering.

Response and Reporting Decision Analysis. Decision analysis tools should also be developed to permit each industry segment to minimize response time and cost and to provide real-time reporting to appropriate organizations. These capabilities would help industry detect and potentially thwart coordinated or interdependent incidents. Because the existence of such decision analysis tools could actually increase risks (and the systems could become the targets of terrorists or disgruntled insiders), they must be developed with integral security considerations.

The overall goals for developing these decision analysis tools are to minimize damage, disruption, and cost of incidents of any kind on the gas and oil energy production and delivery system and to allow immediate response by national security and law enforcement agencies to terrorist or other illegal attack on the infrastructure. Specific goals include the following:

- Provide real-time interpretation of system monitoring sensors.

- Ensure full integration with risk management models and all automated operating data.

- Incorporate accurate modeling of the system interconnections and interdependencies.

- Include an automated ability to order rapid acquisition of additional information such as satellite photos, the news media, and rapid response industry crews.

- Integrate communications with emergency response, law enforcement, and national security agencies.

- Include the capability to determine trends in incidents over time.

- Incorporate an element to resist tampering.

Rationale for the Research and Desired Results

Predictive risk management is an effective method for effectively allocating limited industry and government agency funds to minimize risks. Existing processes in the oil and gas industry, while effective in the past, have entered a period of increasing threat, while operating budgets are increasingly under pressure. Physical threats are generally known to the industry segments, but complexity and interdependencies are increasing their potential impact. Currently, most incidents that result in physical damage are managed as singular events, and response abilities and time vary greatly. Cyber attacks and incidents represent a new threat to the industry. Currently, protection from such incidents is provided by standard computer system "firewall" technology. The current approaches no longer adequately protect this critical infrastructure from the growing potential threat.

Finally, some important scientific advances have occurred in monitoring, sensing, and detecting critical conditions. Many of these advances are beginning to enter the gas and oil industries. However, the decision analysis tools to use the new data effectively and to integrate existing data with new sources have not been developed. Development of such tools can be justified on both economic and security grounds.

Timeframe and Resource Requirements

Predictive Risk Management. As noted, predictive risk management models are needed for each sector of the gas and oil industries. At a minimum, models are needed for gas and oil production; oil refineries, gas processing plants, liquid pipelines, high-pressure gas transmission pipelines, underground gas storage facilities, receiving/storage facilities for petroleum liquids, LNG terminals and storage facilities, petroleum products distribution, and medium- and low-pressure gas distribution networks. Development efforts on these models can be parallel or prioritized following completion of the vulnerability and physical protection assessments described in Sections 3.2.1 and 3.2.3. DOT-funded efforts to develop partial risk management models are underway for liquids and high-pressure gas transmission sectors. These efforts should be continued and expanded to include cyber threats. After all sector models have been developed, an assessment should be made as to the need for, benefits from, and costs of an enterprise-wide risk management model.

Activities for each sector model include the following:

- Assess all available historical data on system cyber and physical components.
- Assess available operating data and its time availability (e.g., monthly, daily, real time).
- Assess available monitoring and inspection data and their time of availability.

- Assess available environmental data (e.g., weather, earthquake) and their time of availability.

- Develop a spatially/geographically based software platform to depict historical and current physical, operating, and inspection/monitoring data.

- Develop expert system models capable of interpreting time change sequences in data, comparing historical with current data, and evaluating environmental data to provide decision-making outputs, including operational changes and maintenance/repair schedules; efforts during this stage of activity will also highlight the need for improved data or information and identify needed capital improvements.

- Demonstrate models over a sufficient time to show that improved safety and security have been achieved at minimum cost.

Response and Reporting Decision Analysis. As in risk management, response and reporting decision analysis tools should be developed for each industry sector either in parallel or by priority. While response and reporting models can be developed without a comprehensive risk management model, the results will be greatly enhanced if both models are developed and fully integrated. Full achievement of the goals stated above requires such integration.

Activities for each sector model include the following:

- Assess available disruption/incident/tampering detection/identification data and their time characteristics.

- Characterize likely damage or disruption.

- Describe response alternatives.

- Delineate all reporting and communications requirements and channels.

- Study human interface elements of the overall response and reporting system.

- Develop an expert system model capable of (1) evaluating available system data and comparing those data in real time with probable conditions during disruption, and (2) providing response outputs (requests for additional information, warnings, or automatic communications as appropriate) necessary to meet the goals stated above.

- Test and evaluate the model, including simulation of potential incidents.

- Deploy and demonstrate the model and its integration with human elements of the industry sector.

- Develop an incident tracking and trending model.

Decision analysis tools for predictive risk management and response/reporting can be developed, tested, and deployed for each industry sector in three to five years at an estimated cost of $3 million to $8 million, depending on the complexity of the industry sector. If both risk management and response/reporting models are developed in parallel for the 10 sectors listed below, the effort could be completed in five years at an estimated total cost of approximately $120 million. An alternative approach would be to develop the five highest priority sector models first, followed by the lower priority sectors. As discussed above, sectors would be prioritized following the completion of the vulnerability and physical protection assessments (Sections 3.2.1 and 3.2.3). Taking this path, completion would require 10 years at approximately the same total cost. The roadmap described below is based on taking this development path.

Finally, after individual sector models are completed, it would be appropriate to assess the need for enterprise-wide models. This resource estimate does not include the cost of such an assessment or of the model development efforts.

The industry sectors and a preliminary assessment of decision analysis model complexity are given in Table B.3.

A roadmap of input for decision analysis models has been developed for the five most important industries. The roadmap identifies goals and groups them by the year targeted for achievement: 2000, 2005, and 2010. They are listed in the subsections below.

Table B.3 Assessment of the Complexity of Decision Analysis Models by Industry Sector

Industry Sector	Complexity
Gas and oil production	Low
Oil refineries	Medium
Gas processing plants	Low
Liquids pipelines	Medium
High-pressure gas transmission pipelines	High
Underground gas storage facilities	Low
Receiving and storage facilities for petroleum liquids	Medium
LNG terminals and storage facilities	Medium
Petroleum products distribution	Low
Medium- and low-pressure gas distribution networks	High

Roadmap Target: Achieve by ~2000

For the five most important industry sectors, initiate work on the following tasks:

- Assess all available historical, operating, monitoring/detection, and environmental data capabilities.
- Develop a spatially/geographically based software platform to depict historical and current physical, operating, and inspection/monitoring data.
- Assess available disruption/incident/tampering detection/identification data and its time characteristics.
- Characterize likely damage or disruption conditions.
- Describe response alternatives.
- Delineate all reporting and communications requirements and channels.

Roadmap Target: Achieve by ~2005

For the five most important industry sectors, initiate work on the following tasks:

- Develop expert system models capable of interpreting time change sequences in data, comparing historical with current data, and evaluating environmental data to provide decision-making outputs, including operational changes and maintenance/repair schedules; efforts during this stage of activity will highlight the need for improved data or information and identify needed capital improvements.
- Study human interface elements of the overall response and reporting system.
- Develop an expert system model capable of evaluating available system data, making real-time comparisons with probable disruption conditions, and providing response outputs — requests for additional information, warnings, or automatic communications as appropriate — to meet the goals stated above.
- Test and evaluate the response model, including simulation of likely incidents.
- Develop an incident tracking and trending model.
- Complete the assessment and characterization activities listed for achievement by 2000 for the highest priority sectors.

Roadmap Target: Achieve by ~2010

For the five most important industry sectors, complete the following task:

- Demonstrate and verify both predictive risk management and response/reporting decision analysis tools.

For the five very important industry sectors, initiate work in the following areas:

- Develop expert system models capable of interpreting time change sequences in data, comparing historical with current data, and evaluating environmental data to provide decision-making outputs, including operational changes and maintenance/repair schedules; efforts during this stage of activity will highlight the need for improved data or information and identify needed capital improvements.

- Study human interface elements of the overall response and reporting system.

- Develop an expert system model capable of evaluating available system data, making real-time comparisons with probable disruption conditions, and providing response outputs — requests for additional information, warnings, or automatic communications as appropriate — to meet the goals stated above.

- Test and evaluate the response model, including simulation of likely incidents.

- Develop an incident tracking and trending model.

3.2.3 Physical Protection Assessment

Description

This research topic will result in a comprehensive assessment of the physical assets of the gas and oil industry, the points of physical exposure, current protection methods, and strategies for future protection. The assessment will cover 10 industry sectors:

- Gas and oil production

- Oil refineries

- Gas processing plants

- Liquids pipelines

- High-pressure gas transmission pipelines

- Underground gas storage facilities

- Receiving and storage facilities for petroleum liquids
- LNG terminals and storage facilities
- Petroleum products distribution
- Medium- and low-pressure gas distribution networks

Goals and Challenges

The goal of this activity is to complete a comprehensive report that achieves the following:

- Statistically based numerical counts of the components of the oil and gas industry physical system (e.g., onshore and offshore wells, gathering lines, dehydrators, compressors, processing plants, receiving terminals, storage facilities, city gates, valves, regulators);
- Specific identification of areas of high concentration of physical facilities (e.g., processing plants, refineries, oil/LNG receiving terminals, pipeline "hubs");
- Characterization of current protection methods used by the industry; and
- Determination of advanced protection methods and an analysis of the costs and benefits for the application of these methods.

Rationale for the Research and Desired Results

No comprehensive study of the physical assets of the gas and oil industry has been compiled. Government (DOE/EIA and U.S. Department of the Interior) data requirements and industry databases provide a partial, but incomplete, picture of industry assets. No analysis of current and potential advanced protection methods is available.

Timeframe and Resource Requirements

The following tasks are required to assess the physical assets of the gas and oil industry. A roadmap of input for these assessments has been developed. The roadmap identifies goals and groups them by the year targeted for achievement. The goals are listed below. The resource requirements in the near term are estimated to be $5 million.

Roadmap Target: Achieve by ~2000

- Conduct surveys and statistical analyses to fill the gaps and to upgrade existing data.
- Collect existing data from government and industry sources; determine whether the data are adequate and identify existing gaps.

- Analyze the data to determine the points of concentration and vulnerabilities of the physical facilities.

Roadmap Target: Achieve by ~2005

- Survey the industry to determine the protection methods currently being used for areas identified as highest concentration and vulnerability.
- Conduct a technology assessment of physical protection methods.
- Develop strategies for use of advanced protection methods in the oil and gas industry.
- Analyze the costs of and benefits from using enhanced, advanced methods.

An additional task to be completed by 2005 is to publish the study.

3.2.4 Multisensor and Warning Technologies

Central to the protection of any infrastructure is the implementation of an integrated, corroborative system of overlapping technologies designed to warn against intruders at any of the critical facilities and control nodes along that system. The proposed integrated Multisensor and Warning Technologies (MSWT) system would further facilitate analysis of data to provide information that can be used to anticipate attacks and identify perpetrators.

The most critical of such facilities and control nodes in the gas industry include:

- Interstate pipelines,
- Compressor stations,
- City-gate stations,
- Odorant injection sites,
- District regulator sites,
- Any pressure or flow control site,
- Gas control centers,
- Remote metering sites,
- SCADA control centers,

- Any SCADA-driven controls, and
- Any site that intersects with other vulnerable infrastructures.

Description

Industry and government research and operating personnel would evaluate leading technologies for immediate development and commercialization. Initially, they would focus on tamper detection and failure warning technologies for remote locations, including acoustics, electronic signals, biological and chemical toxin sensors, video-imaging, satellite oversight with GPS systems, remote methane detection, expert system predictive methodology, and SCADA communications and control standards.

Goals and Challenges

The most important element of this analysis is determining whether the identified tamper detection and failure technologies are both scientifically sound and operationally practicable. The leading technologies in each of these areas would be analyzed to determine whether the industry was likely to view them as commercially justifiable in terms of the benefits they could bring in today's highly competitive world. Those technologies that are most beneficial from a commercial viewpoint would have a preliminary advantage over technologies viewed as noncommercially productive.

Rationale for the Research and Desired Results

The approach described above is necessary because industry will be reluctant to spend money to guard against potential emergencies, unless it can see a payback on an ongoing basis from a business perspective. When properly implemented, through the combined resources of government and industry, this strategy will result in a profoundly more robust infrastructure, more accessible to open-access commerce and trading, yet far less accessible to sabotage or terrorism.

Scientists, engineers, and industry operating personnel will review the selected technologies. They will establish the best way to link the strongest technologies into one integrated intrusion warning system. This system will communicate attempted intrusion at any site along the infrastructural system and then automatically verify the attempt by querying another independent technology. For example, if an acoustic sensor placed along a pipeline were to detect a variation in the sound of gas flow through the pipeline that was not explained by electronically monitored valve settings, it would automatically call for backup verification of leakage or sabotage from a satellite with remote methane detection capability or an electronically driven pattern-recognition system.

Software and hardware additions to existing commercial products that must be added to make the warning system fully functional will be developed in partnership with government oversight and relevant technologies developed within both government and industry laboratories.

The system must also be designed to immediately deliver a real-time warning to the gas control centers and emergency response centers of the involved gas companies. In addition, the system must warn the control centers of intersecting infrastructures such as electric power control centers, so that they can take appropriate mitigative actions. It is crucial that at least two intrusion warning technology systems are in place at each site so that the two technologies can validate each other's findings in real time. This dual-technology approach greatly reduces the ability of a saboteur to "spoof" one technology or another, which would result in incorrect response measures.

In addition, the intrusion protection system must be interpretive and integrated. In this sense, interpretive means that results from the sensor outputs will be examined to determine whether they fall into temporal or geographic sequences of events that indicate an actual threat. At the site level of a physical assault, for example, a sequence of events consisting of a video image of a person climbing a fence, followed by detection of a door being opened, followed by a change in a set-point would be assigned a much higher threat potential than a single door opening. The warning, in other words, would be increased based on interpretations that the sequence of events in the example accords with a pattern expected for site penetration. The same sequence analysis would be performed and fine-tuned to protect against cyber assault. The system will be interpretive in that it will collect security data in a central repository for further analysis. Both the cyber and physical detection systems must also be designed to collect information about the individual attempting the intrusion.

In partnership with all sectors of the gas industry, including manufacturers and vendors, the next step is to implement the MSWT physical and cyber intrusion warning system on an operating basis. The partnership of gas industry executives and technical staff is essential to assure that the system is initiated over as large an area of the country as possible, as efficiently and cost-effectively as possible.

The operating expertise and the substantial market power of industry are the most powerful market-building tools here. Large regional gas companies operating in each of four regions of the country will be selected to establish themselves as standard-setting and manufacturing/distribution centers for the technologies considered to be most effective for system implementation. These companies will be selected on the basis of market power, integrity of personnel and operations (as determined by an ongoing record of outstanding industry performance), and willingness and capability to manufacture the required hardware and software on a mass basis.

The companies selected will be able to recapture their partnership costs and gain significant profit through sales of the required hardware and software to themselves, their subsidiaries, and the smaller gas companies in their service territory who wish to share in the economic and security advantages of participating in the intrusion warning system. This significant manufacturing and vending opportunity will strongly encourage all involved to place their considerable marketing power and expertise behind the project, thus expanding the market at a rapid rate to include the entire country within a short time.

This plan will reduce government spending, while, at the same time, garnering strong industry support for this crucially important project.

Timeframe and Resource Requirements

It is proposed that a 10-year program be put in place beginning in 1999. The purpose of the program would be to fully plan and evaluate, design the hardware and software for, and then implement an infrastructure-wide intrusion warning system that covers all these critical points and others within the infrastructure. The plan is envisioned to take place in three carefully defined phases, each running a set number of years with carefully designed end-points and deliverables that lead into the next phase.

The near-term deliverable, as outlined above, is an extended report on technologies analyzed, architecture recommended for system design, and analysis of technological gaps that remain in the system. The last will require additional hardware and software development and an explanation as to why those additions are required. The report will be distributed to relevant government and industry review parties and be released as a formal guideline objective**.** The starting and completion dates for Phase 1 are September 1998 and August 2000. The approximate cost is estimated to be $20 million over two years.

Phase 2 involves a comprehensive description and roadmap of an accepted infrastructure intrusion warning system based on multiple verifying technologies. It may be necessary to add software and hardware to make the independent technology systems capable of reliable and hardened communications at all times, once the full system has been implemented. Starting and completion dates for this phase are September 2000 and August 2005. The estimated cost of Phase 2 is $40 million over five years.

Phase 3 is commercial deployment or implementation. The commercially available physical and cyber intrusion detection system will be deployed or implemented across one or more major regions of the country in cooperation with the largest gas companies. Full market expansion forces will be at work throughout the nation. An industry/government investigative committee will continue to oversee potential vulnerabilities of new operating facility designs and analyze them to determine whether additional sensors or other warning technologies should be incorporated. The starting and completion dates for Phase 3 are September 1998 and August 2010. The estimated cost is $100 million.

3.2.5 Emergency Response Capability Enhancement

Description

Natural gas and oil companies have emergency response plans to use in times of crises. Each company’s plans are unique and typically are not shared among industry and government. However, help is provided informally during crises, as companies contact other companies for assistance. Historically, the gas and oil industries have been tested

with various emergencies and have responded well. However, these industries are downsizing, while additional threats, such as cyber threats, are surfacing. Little formal assistance within the industry or within the federal government is available. A formal emergency response plan could provide additional assistance to these industries as needed.

This topic focuses on what can be done to change our natural gas emergency response procedures. Potential changes include identifying formal communication channels during crises, establishing protocols for these communication channels, identifying what industry and government assistance should be provided, and deciding what best practices should be implemented in this area. Also included is an R&D technology plan to assist industry during crises; specifically, increased development in technologies such as portable compressor stations, portable gas supplies (e.g., compressed natural gas [CNG] trailers), quicker pipeline repair techniques, and city-gate station repair, which could play an important part in mitigating the impacts from these emergencies. Federal ownership of gas supplies in storage or development of new storage capacity are other options. Also, changes in policy and regulations would be needed to create a formal national response plan.

Goals and Challenges

The major goal for examining emergency response is to allow industry to be better positioned to respond to crises, from either natural or man-made disasters. Minor disruption of gas and oil supplies can cause economic hardship to businesses and individuals; it even threatens life itself, as many people require gas or oil to provide heat during winter months.

Challenges to this research topic arise in several areas. Deregulation pushes companies to focus more on profits and less on emergency procedures. Companies are sometimes hesitant to work with other companies for fear of divulging proprietary information. Anti-trust laws also discourage company discussions. Each gas and oil system is unique, which makes it more difficult to determine what can be done at a national level. A large representation of companies would be needed to ensure that a range of vulnerabilities is addressed.

Industry is reluctant to involve the government for fear of increased regulation. It will take time to develop the necessary communication channels between industry and government. It is important, however, to involve the government. The government must create a level playing field so that all companies participate to a certain minimum level. This level should be developed jointly, with heavy industry involvement. The government also has vast resources of expertise that could be tapped to assist companies in emergencies.

Rationale for the Research and Desired Results

The natural gas and oil industries face emergencies from natural disasters, physical sabotage, and cyber attacks. These occurrences have the potential to disrupt service of gas and oil supplies for extended periods. Minimizing the time needed to restore service is paramount in lessening damage from these disruptions. These industries have an excellent track record during crises; however, new constraints and threats are being introduced.

Companies must operate their systems at higher capacity, with less staff, and with reduced operational budgets. Much equipment is available during crises, but budgets prevent companies from maintaining all the equipment needed. A possible solution is to have an industry pool of resources combined with a government pool of resources. An industry/government partnership would examine both the need for equipment/staff during crises and the need for potential measures that could help mitigate these crises.

The government has many resources that can be used during emergencies: stockpiles of necessary equipment, such as pipe, valves, and compressors, as well as portable equipment, such as portable compressor stations, pumping stations, and CNG trailers that hook into gas pipelines. For oil, the Strategic Petroleum Reserve is one mechanism currently in place to mitigate the effects from a disruption in the oil supply. For gas, government ownership of gas supplies in storage could be considered, as could development of additional storage capacity.

An industry/government partnership could help determine where R&D dollars should be spent in this area. Together, both entities could identify and prioritize vulnerabilities. From that list, they could begin to map an R&D plan that could be a template for cooperation toward mitigating the impacts from these vulnerabilities.

Timeframe and Resource Requirements

In the near term (end of 2000), the industry/government partnership would be established. The partnership would begin to identify roles and any technology gaps for R&D projects. Between 2000 and 2005, R&D dollars could be allocated, with some technology implementations starting during this period. By 2010, technologies and best practices would be widely implemented within the industry. It is estimated that this near-term (end of 2000) effort would cost $2 million. The costs for efforts between 2000 and 2005 are estimated at $50 million, and the costs for efforts between 2005 and 2010 are estimated at $100 million.

3.2.6 Cyber Protection Enhancement

Description

SCADA systems contain all information and control elements, including flow control devices that can be remotely or automatically triggered via microelectronic signal.

Systems are as robust or as weak as their weakest remote-accessed element. The record-keeping capabilities and physical control capabilities of such systems are increasingly being integrated.

The natural gas industry's electronic commerce and SCADA systems are increasingly being linked to each other and are therefore becoming more vulnerable to cyber intrusion. The speed with which such vulnerability increases is driven by the economics of competition under open access, where all companies must operate their SCADA systems by means of widely published standards of communication. These standards, and the access they provide outsiders into corporate computer centers, increases the probability of malicious access not only to financial and other operating records, but also to SCADA-driven controls.

The industry must develop a viable method to economically enhance the security of these systems, reversing the trend toward greater vulnerability.

Goals and Challenges

The degree of linkage between commerce trading requests and direct SCADA physical control centers that fulfill those requests is likely to accelerate rapidly because such direct interaction enhances the speed with which a transaction can be processed. As a result, more transactions can be processed per day, which leads to a greater flow of dollars into the company. The speed of linkage must be improved, while maintaining the integrity of the system.

Industry is tending toward bringing the standards for commerce and SCADA communications closer together. While this trend enhances the ease of transactions, it also adds to vulnerabilities because outsiders can more easily access (and cause damage to) multiple sites and even multiple companies across the nation simultaneously.

The gas industry is not yet fully aware of this increasing vulnerability. As a result, the industry has become increasingly susceptible not only to major financial sabotage, but also to the manipulation of physical controls through cyber intrusion. This vulnerability creates the potential for significant physical damage to industry facilities and urban centers through the remote intervention of outside parties who are familiar with industry operations and communications codes.

If these trends continue unabated, without protective measures such as encryption being taken to safeguard the integrity of the cyber system driving these transactions, it is easy to envision a scenario of grave proportions. Outsiders could stage an attack and simultaneously take control of the SCADA systems, which control pressures at critical sites in numerous urban centers and military installations. Such an attack could lead to a cascade of failing pressure and a major disruption that would cut across electric power, financial, governmental, and other infrastructures at a critical time.

Rationale for the Research and Desired Results

An industry-government partnership is critical for success in creating and implementing appropriate encryption and other safety standards that will enhance the speed and security of commercial transactions, while significantly strengthening the infrastructure and making it less vulnerable to cyber attack. Cooperation between industry and government scientists and engineers greatly enhances trust and acceptance, and assures the effectiveness of the operating units as they are put into the market. This partnership should include such groups as the standards-setting committee that is working toward an open architecture with communication standards.

The objective is to create an open architecture that has the necessary flexibility to allow for the unique needs of multiple system users and vendors, yet one that will still provide full protection against a large-scale cyber assault. These systems and codes can be designed to allow quick access to the electronic commerce gateways required for ease of open-access trade, yet block the interior encodings that drive the physical components of the SCADA system. This capability could be developed in a three-phase cooperative effort.

In Phase 1, the partnership entity would design and identify appropriate encryption algorithms that would make it extremely difficult for any outside party to access the industry computer data banks beyond those that record commercial transactions. A search of COTS and government off-the-shelf (GOTS) products would be performed initially to leverage off of existing research.

Phase 2 would incorporate these encryption systems and other devices onto computer chips that can be attached to all commercial-transaction units as well as all SCADA-driven control units. These chips would verify the integrity of messages sent to those units. Ongoing communications, laboratory work, and product verification are required for each manufacturer's SCADA system, along with separately configured SCADA components for each manufacturer to assure full compatibility and communications capability with the rest of the systems on the market. The manufacturing design of each component must be further investigated under field and laboratory conditions to ensure that adding encryption chips or other electronic protective devices does not interfere with the unit's operational quality. Without such attention to detail, one or more operating controls or critical data nodes within the SCADA system would go unprotected. Because any comprehensive SCADA system is only as strong as its weakest link, that unprotected link could allow an intruder to enter the overall system.

Because the design mechanism for each of these controls is unique from one SCADA element to another, coordinated industry participation is essential and must include operating experience, the leading manufacturers and vendors in the gas industry and the large transmission and distribution companies themselves to assure that each chip is properly attached in a functional mode.

The goal for Phase 3 is to have an Enhanced Cyber Protection System for SCADA and electronic commerce running in major regions of the country. To accomplish this task requires taking the standards and prototypes developed in Phases 1 and 2 to the largest regional gas companies in each section of the country. These companies would act as proponents of the system and manufacturers/vendors of system components.

The industry-government partnership would also promulgate a set of security protection standards that all future SCADA units and components would be required to meet. These standards would ensure that despite the unique features devised by individual vendors in the future to enhance continued commercial advances, the units would remain protected against cyber assault.

Close work with industry participants is required in this phase to help them recognize the opportunities and profits to be made by accepting and adhering to these standards. Not only will the acceptance of these standards guard the industry against cyber assault, but it will also standardize signals that provide a gateway to the entrance of each manufacturer's system components. In this way, companies can guard against the possibility of incurring huge overall system replacement costs they might have incurred if their chosen SCADA component manufacturer goes out of business and cannot replace units or expand existing system coverage.

Timeframe and Resource Requirements

Phase 1 will result in a comprehensive report on the design of the above-mentioned encryption and corporate-address identification standards that can be used for commerce and SCADA control systems, as verified by government oversight. These standards are further to be accepted as realistic, practicable, and useful by the industry as evidenced through industry committee acceptance and the beginning of work toward implementation of the suggested system. The start-up and completion dates are September 1998 and August 2000, respectively. The estimated cost is $1 million.

In Phase 2, researchers will review current hardware and software security measures, along with operationally practicable chips, for proper encryption and protection methodologies for all existing major data and physical control units that form a significant share in SCADA system and electronic commerce. In addition, a prototype will be manufactured. The start-up and completion dates are September 2000 and August 2010, respectively. The estimated cost is $100 million.

In Phase 3 the new technology and standards will be deployed. These are to be fully accepted by industry by September 2010, with commercial implementation of the EPS underway at that time. The start-up and completion dates for this phase are September 2000 and August 2010, respectively. The estimated cost over the full scope of the task is $100 million.

3.3 Joint Topics

3.3.1 Evaluation of Policy Effects

Description

Many potential vulnerabilities of a system can be averted by having appropriate public policies in place. However, some policies can have a very detrimental effect on the vulnerability of the grid. Because it is important to understand these relationships, the following tasks should be performed:

- Study any cause-and-effect relationship between the degree of vulnerability of a system and laws, directives, operating policies, and standards.
- Understand the effect of financial incentive and/or tax policies on security.
- Develop the means for accurately assessing vulnerability so that policies that address vulnerability issues are more specific.

Conversely, it is reasonable to assume that appropriate policies can reduce system vulnerability.

It is important to understand the relationship between financial incentives and creation of robust, reliable, disaster-resistant energy infrastructures. Without the proper incentives, implementation of measures to provide such infrastructures will be limited and haphazard. The very substantial financial investments required to develop these infrastructures and long asset lifetimes also argue for careful attention to this topic. Because establishing such incentive structures is often an issue of contention, and because reliability of complex infrastructures is difficult and challenging, it is imperative that this topic be given considerable attention in a collaborative and cooperative industry and government program.

Goals and Challenges

Goals and challenges for policy implications on security include the following:

- Understand all the connections between a policy and its effect on system vulnerability.
- Understand any trade-offs between system security and cost. Develop policies that improve the economic welfare but also consider system security.
- Develop policies that provide adequate economic incentives or regulatory mechanisms to ensure prudent construction and operation of energy transmission facilities.

Rationale for the Research and Desired Results

Energy infrastructures are complex and largely privately owned, but system failures can have widespread implications for the nation as a whole. An appropriate public policy must balance the needs of private enterprise against those of individual consumers and the nation.

Relying exclusively on private efforts to address vulnerability problems can result in promotion of self-serving policies and the adoption of specific technologies that are not in the best interest of society. Relying exclusively on government efforts can stifle creativity. Balance and cooperation are needed.

Appropriate policies can lead to situations where less vulnerable systems are the natural consequence of normal business practices. The converse is also true.

Implementing appropriate policies provides the opportunity to internalize environmental and other externalities. An understanding between environmental policies and network vulnerabilities is important.

Relating policies to good objective engineering criteria is essential. Several elements of an electric power grid make it quite unique and may require creative new types of policies and laws.

Narrow vested interests on the part of specific groups (regulators, conventional utilities, power marketers, and others) can lead to policies for system construction and operation that are detrimental to the system, and under some conditions, lead to large-scale disruptions. In particular, it is essential to all parties who have influence into these policies to recognize that the power system of the future is less constrained by state or company boundaries than it is by the physics of the grid.

Public policy can have serious long-term consequences. Once a policy has encouraged the construction and deployment of a given technology, we are generally bound to live by that technology for many years. Thus, it is important that public policy be directed appropriately.

Another key role for public policy is to address environmental factors. It is important that public policy recognize any effects on the environment.

Timeframe and Resource Requirements

A strategy for attaining the research goals includes creation and fostering of efforts intended to train individuals with broad backgrounds, who can understand both the technological aspects of a problem as well as associated policy issues.

Research intended to ascertain the economic impact of any regulation, policy, or standard before and after it is enacted is important. The implications of such a decision on the welfare of specific interested parties and the interests of society at large are important.

Furthermore, an independent investigation of alternative industry and system structures should be performed. This investigation should include research on means to make the power system less brittle and less complex. It is essential that such an investigation be conducted by reasonably independent groups from a variety of viewpoints, rather than merely as a direct extrapolation of present practice. This exercise will take place regardless of any research activities undertaken. What is needed is an investigation of fundamentally different policies that may lead in different directions for a more efficient evolution of the industry, but that would have been overlooked by individuals whose main concern is the next round of decisions or the next quarter's performance.

The budgetary and project recommendations in this area are organized into several categories:

- Investigate the effect of numerous proposed or conceivably proposed policies on the vulnerability and security of the system. An effort on the order of $1 million per year for three years would be appropriate.

- Explore the implications of operating the grid as a single, integrated grid to which participants connect (the highway system analogy) compared with operating privately owned grid structures. Do so by performing comprehensive studies of various alternatives. The estimated cost is $3 million per year for three years.

- Study the implications of allowing independent standard-setting bodies to establish guidelines and standards for system design and/or operation. The other alternative is to allow industry groups with specific interests to be in charge of these matters. This category is very timely and highly urgent, and it is recommended that $1 million per year be allotted for these studies for two years.

- Encourage the creation of educational programs that lead to graduates who are knowledgeable in both technical and public policy issues. Appropriate grants to selected universities to foster this type of activity would be welcome. A suggested level of funding is for eight institutions at $250,000 each (on average), for a total of $2 million per year for five years.

- To lead to a more informed set of decisions, engage in investigations of the social costs associated with various possible outages and other vulnerabilities of the grid, including fuel supply and other nongrid disruptions. Suggested spending is $1 million per year for five years.

- An understanding of power market issues in electric transmission is far from resolved. A three-year, $2 million per year effort is suggested to address vulnerabilities that can

result from power market concentration, including perhaps new theoretical and experimental work on power market issues.

3.3.2 Institutional Barriers

Description

This research topic focuses on institutional issues that are potential impediments to the successful implementation of the Commission's strategic and technical objectives. A number of these issues have surfaced in activities following the release of the Commission's report. For example, the need to establish a joint industry-government partnership became apparent during an Information Assurance Wargame held at the Army War College in February 1998. The initial research activities are predominately analytical and directed at characterizing the issues and options.

This research affects a spectrum of Commission activities, particularly the process of implementation. Accordingly, it is based more on the disciplines of policy and operations research than on technological disciplines.

The result of this research and analysis is a series of plans that recognize and address the potential strategic, policy, and structural constraints facing an initiative that embraces national coordination and alignment to a common set of priorities. The plans may include operating charters in which teams are either involved or proposed.

Goals and Challenges

The Partnering Model. Development of partnerships is based on joint pursuit of a specific concept or model of how the partnership is structured, and the respective roles, responsibilities, equities, and resource requirements. A shared vision of the model is critical, yet rarely exists at the initiation of discussions. Excellent examples of these comments already are evident within the Commission initiative.

This research area supports the development of these partnerships. It is concurrent with the partnering process and plays a supporting role, and in some instances, may serve a host function in the process. The partnering model should be established by government-industry teams from the respective infrastructure areas. There will be multiple teams, each with its own model, because the industries are not homogeneous with regard to need or culture.

A significant challenge will be to obtain the appropriate representation on the teams to achieve successful partnering. The specific goals of the team must be defined. The focus should be on characterizing the needs and implementing the appropriate infrastructure to support each industry. A host, or supporting function, for each team, preferably familiar with the respective industries, will be necessary to implement the teams' directions.

Basic Tools. The partnering concept depends on mutual industry and government agreement on key issues such as the threat to the infrastructure and the need to address it. An implicit assumption is the dedication of resources. At the present time, however, the effort is primarily driven by the government's concern with regard to national security. Industry is, for the most part, resigned (if not content), with the status quo. Therefore, communication and implementation "products" must be developed to foster recognition of the threat and means to address it.

For example, one objective is to foster enhanced cyber threat security in firewalls and SCADA systems. Therefore, success depends on:

- Individual companies concurring with the premise that the threat is significant and imminent, and

- Availability of firewalls superior to those that the companies are using.

This effort presents a host of barriers because the threat has not been adequately characterized, and there are no recognized uniform standards, or even metrics, to rank the security effectiveness of various firewall products.

The product needs to consist of (1) a package of specific examples that characterize the threat sufficiently to enable consideration of new defenses or at least evaluation of the existing defense, and (2) development of standards and test protocols that enable comparative evaluation of various security mechanisms.

Leveraging Existing Infrastructure. The enormity of the task outlined in the Commission's report is apparent. Not only must the essential message be communicated and embraced by infrastructure operating units and their respective government agencies, but plans, resources, and actions must ensue. The diversity of needs adds to the challenge.

Each of the critical infrastructure industries has organizations that serve the industry in various capacities, from R&D management to lobbying and marketing. Understanding the roles of these organizations and leveraging their existing networking and understanding of their industry are advantageous from a time- and cost-effectiveness standpoint. Strategic alliances may be formed that can help to bridge the formidable cultural gap between government imperatives and industry priorities.

There is an added complexity of focusing on domestic infrastructure within multi-national companies that increasingly minimize the implications of national boundaries. Particularly in the oil industry, it is important to recognize that additional security that emphasizes U.S. domestic boundaries can impede normal business operations, which are not constrained by these boundaries.

Rationale for the Research and Desired Results

The requirements for heightened security of the national critical infrastructures are very broad and cut across industrial, governmental, policy, technological, and financial issues. Therefore, conflicting priorities that arise must be resolved before the Commission plan can be successfully implemented.

Take, for example, crosscutting policy/financial issues. The backbone of the Commission recommendations is based on a "partnering" between industry and government, which requires resource investments from each. It is not clear, however, where the line is drawn to distinguish between national security priorities that should be supported by the government, and corporate governance that should be supported corporately. This fact influences the respective resource investments.

Furthermore, some of the governmental agencies earmarked for partnering also have a regulatory function. Industry has a traditional perspective that regulators "live to regulate" and to expand their authority. To establish a partnering relationship, it is necessary to clearly identify the nature and objectives of the relationship. Alternatively, other structural approaches to the partnering arrangement can be examined.

Such issues are subtle, yet effective barriers to achieving a successful merger of objectives between organizations of any type. Understanding and addressing such issues is a prerequisite to success. Within the context of the Commission initiative, three areas of potential actions are apparent: (1) the partnering model, (2) basic tools, and (3) leveraging existing infrastructure.

Timeframe and Resource Requirements

The Partnering Model. The plans for establishing a partnership would begin by forming a gas, oil, and electric team by April 1999, with final plans in place by December 2000 and implementation by 2002. The budget is estimated to be $900,000 per year for 1999 and 2000. This amount covers leadership and coordination, fact finding, analysis, and logistical support.

Basic Tools. The tools needed for the initial planning phase would be in place by December 1999, with subsequent plans in the following three years. The deliverables depend on the product or tool. The budget is estimated to be $2 million for 1999 and $5 million per year for 2000 through 2004. These funds would be used for analytical support for this phase.

Leveraging Existing Infrastructure Support. The budget for infrastructure support of outreach and operations activities is estimated to be $500,000 to $900,000 per year per industry for five years. The outyear budgets depend on the operating structure within the industries to maintain the support and networking needs, such as the Federal Bureau of Investigation security center.

3.3.3 Infrastructure Interdependencies

Description

The Executive Order that created the Commission determined that certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These infrastructures include electric power, gas and oil production and storage, banking and finance, telecommunications, transportation, water supply, emergency services, and government services.

Procedures related to normal operations, response to an incident, and recovery for any one of these infrastructures typically assume that services from other infrastructures would be available for support. The electric power infrastructure is critically important for operating other infrastructures. Each infrastructure depends to varying degrees on electric power for systems and facilities, as well as emergency backup power. For example, power outages affect virtually every mode of transportation, including subways, elevators, and street traffic (no traffic lights or gasoline pumps). Another important example is the dependence of computers and computing systems on electric power.

On the other hand, the energy infrastructures depend strongly on computers and computing systems for operations and communication. The energy infrastructures also depend on the oil and gas production and storage infrastructure and on the transportation infrastructure for delivery of fuel, including coal, which supplies more than one-half of all electric generation. The energy infrastructures also depend on the other critical infrastructures for financial services and transactions, water supply, and emergency and government services.

Another type of interdependency that may become more prevalent in the future is two infrastructures sharing the same component, such as an energy utility sharing the same cable with a telecommunication utility. This new interdependency will be driven by the needs of the deregulated electric utility sector to control costs by deploying both supply-side information technologies and demand-side energy information services. These information services will enable utilities (1) to provide higher-quality services at lower cost with lower environmental impact and (2) to give their customers better control over their power usage. The excess capacity on these lines could be sold or leased to information services providers.

Other examples of interdependencies that need further examination include:

- The impact of decreases in electric power quality on communications and computing;
- Widespread use of electric vehicles on transportation and electric power;
- Remote control mechanisms and communication for improved gas distribution network performance when electric power is not available;

- Small, reliable, efficient gas-driven generators to reduce dependence on electric power for gas delivery and utilization;

- Energy conservation devices on electric power network security and telecommunications; and

- Increasing dependence of the electric sector on natural gas.

A high priority identified in the Commission's report, *Critical Foundations*, was to conduct R&D in this area:

> Advanced methods and tools for vulnerability assessment and systems analysis are needed to identify critical nodes within infrastructures, examine interdependencies, and help understand the behavior of these complex systems. Modeling and simulation tools and test beds for studying infrastructure-related problems are essential for understanding the interdependent infrastructures.

Goals and Challenges

Identification of the existing vulnerabilities and the technical impacts of interdependencies for the energy systems is a challenging first step. Improved understanding of the potential impacts of interdependencies is needed to describe and justify the requirements for modeling and simulation R&D.

Quantifying impacts of the vulnerabilities on the energy system will also be a challenging step and may need to consist of a number of measures. One measure would be the potential loss in dollars to the local or national economy caused by a disruption in the energy system. Another measure would be the time or resources required to mitigate a disruption in the energy system. As the analysis progresses, other measures that need to be considered may be identified.

After quantifying the impacts, a ranking methodology should be developed so that all quantified measures can be considered appropriately. This ranking can then be used to determine those interdependency issues that need attention first. However, some measures may not be easily quantified but may have important impacts. These impacts should not be ignored in the final ranking.

Recent deregulation of some infrastructures and imminent deregulation in others will create new interdependencies in the future (e.g., the telecommunications and electric utility infrastructures). Consequently, another challenge of this research area will be to forecast new interdependencies that may develop and to assess their potential impacts. Because technology can change rapidly, analysis of new interdependencies will be a dynamic process.

Interdependency tools need to address large-scale interdependency issues that affect more than one infrastructure from a technical, economic, and national security perspective. Traditional modeling and simulation tools, while capable of addressing a subset of these issues for a portion of a single infrastructure, are not computationally capable of addressing the complexities and uncertainties associated with these issues on a national level. In particular, the number of infrastructure dependencies and dynamic feedback loops that need to be considered is prohibitively large (i.e., computationally intractable). New computational algorithms and supercomputing capabilities have the potential for efficiently and effectively addressing these modeling and simulation shortfalls. With enhanced computational capabilities, it would be possible to comprehensively address, for the first time, infrastructure dependencies and real-time interactions within a technical, economic, and security framework.

Rationale for the Research and Desired Results

A system description and basis are needed for evaluations of options for prevention, mitigation, response, and recovery. Evaluations should include a comparison of the benefits and costs of introducing the options. The existing framework is too infrastructure-specific and, in most cases, represents only a portion of the infrastructure, let alone any specific dependencies on other infrastructures and the consequences of losing services from those infrastructures.

This research topic would not only improve understanding of interdependencies, but also provide a basis for evaluating the options to address vulnerabilities created or enhanced by the interdependencies. Also, because of rapidly changing technologies, forecasting future interdependencies and projecting their impacts will be important. These forecasts and projections will allow preventive or mitigative measures to be identified early in the process and "built into" the interdependency. This will be a more effective and less expensive way of dealing with the interdependency.

Timeframe and Resource Requirements

Interdependency research topics include the following:

- Methods to relate the technical complexities to business disruptions and economic losses, thereby allowing prevention and mitigation options to be presented and analyzed in a business framework. This task is achievable by 2000 with resource requirements estimated to be less than $1 million.

- In-depth analyses that identify and quantify the technical impacts of the many interdependencies of the energy system infrastructures. This task is achievable by 2000 with estimated resource requirements of approximately $1 million. This effort should be updated periodically to address new developments and changing interdependencies.

- Identification and analysis of options to reduce the effects of interdependency, expressed in the business framework developed earlier. This task would be ongoing and would also benefit from the subsequent modeling and simulation work. Some results would be available by 2000; however, it may be between 2000 and 2005 before thorough analyses can take advantage of the prior work on this topic. The estimated cost is $3 million, with a modest annual updating requirement.

- Examination of the requirements for advanced computational modeling and simulation tools to address large-scale interdependency issues that affect more than one infrastructure from a technical, economic, and national security perspective. This task is also achievable by 2000 with estimated resources of approximately $1 million.

- Development of modeling and simulation tools and their application to improve strategies for reducing the impacts of interdependencies. This task would be ongoing and would result in continual improvement of tools and analysis of options to reduce interdependency-related vulnerabilities. Preliminary results of this effort may be available by 2005, but actual results may not be available until between 2005 and 2010. The estimated cost for this effort over the entire 1999–2015 period is $25 million.

3.4 Summary of Research Topics

Table B.4 summarizes the research topics described in this report. The table addresses the type of research, rationale, research products, goals and challenges, threats and vulnerabilities addressed, and priority category recommended by the Energy Infrastructure Assurance R&D Team. All R&D topics identified in this report are considered well worthy of federal support. If the Energy Infrastructure R&D Team had authority for research funding, all topics identified would be likely to receive some support, even if budget constraints were relatively severe.

Three priority categories are shown in Table B.4: most important, very important, and important. Topics not worthy of serious consideration are not included. In judging the relative priority, the following interrelated factors were considered:

- The extent to which the R&D, if successful, would reduce infrastructure vulnerability, mitigate the impacts, or speed the recovery after a disruption;

- The magnitude of potential consequences that would be prevented or mitigated; and

- The importance of the R&D for national security, the economy, and the social well-being of the United States.

Although the contributors to this report have suggested relative priorities, further study is warranted for many reasons; among them, the short time available for preparation of this report and the several R&D topics that contain a wide variety of research topics at various stages of progress.

Table B.4 Summary of Research Topics

R&D Topic						
No.	Title (Type[a])	Rationale	Product	Goals and Challenges	Threats and Vulnerabilities	Priority Category
1	Real-time Control Mechanisms					Most important
1.1	Instrumentation and Monitoring for Distributed Control (A, ATD)	Enable greater use of existing electrical system.	Hardware and software	G: Share information in real time. C: Develop common data model, sensors and timing, high-bandwidth communication, information exchange.	Physical, cyber, complexity, interdependencies	
1.2	Analysis and Computing for Large-scale Systems (B, A, ATD)	Prevent and recover from large system outages; implement control countermeasures against malicious attack.	Software	G: Measurement-based methods. Detect attempts to disrupt a competitor's position. C: Develop stability indices. Handle uncertainty.	Physical, cyber, complexity, interdependencies	
1.3	Advanced Control Methods (B, POP)	Increase options to prevent or manage outages.	Software, mathematical theory	G: Control large-scale systems. C: Hierarchical control architecture, robust control theory advancements, control methods that use incomplete information.	Physical, cyber, complexity, interdependencies	
1.4	Decision Support Tools (B, A, ATD, POP)	Diagnose problems and sort important information during emergencies.	Hardware and software	G: Develop enabling tool. C: Artificial intelligence, autonomous agents.	Physical, cyber, complexity, interdependencies	
2	Analysis of Scale and Complexity (B, A, ATD, POP)	Mitigate urgent threat or vulnerability; recognize the potentially large consequences of not addressing this threat; common mode failures.	Assessment reports; identify and evaluate incentives	G: Understand complex systems. C: Work after utility deregulation occurs. Develop national security goals for electric grid. Develop incentives to encourage utilities to make necessary investments.	Physical, cyber, complexity, interdependencies	Most important
3	Vulnerability Assessment (B, A)	Assess vulnerabilities and impacts needed to aid decisions regarding research and capital investment.	System vulnerability information, quantification of impacts, method for evaluating options	G: Provide credible information about the performance of the electric power system. C: Assemble methods, tools, and research participants.	Physical, cyber, complexity, interdependencies	Most important

Table B.4 (Cont.)

R&D Topic No.	Title (Type[a])	Rationale	Product	Goals and Challenges	Threats and Vulnerabilities	Priority Category
4	Information Assurance and Cyber Security					Very important
4.1	Threat Assessment and Risk Management (A, ATD)	Tools do not exist.	Tools to help designers of interconnected, market-based system	G: Develop accurate model of electrical system. C: Address vast size and complexity of system and short response time.	Physical, cyber, complexity, interdependencies	
4.2	Large Systems Analysis (B, A, ATD, POP)	Understand large, complex systems.	New models, simulation techniques, integrated attack models, design tools	G: Improve understanding of electrical system. C: Address variety of protocols and legacy systems, validation, technology evolution.	Physical, cyber, complexity, interdependencies	
4.3	High-security SCADA Systems (A)	Changing industry means increased risk to SCADA systems.	Design guidelines, tools, new protocols	G: Protect communications system from attack. C: Add encryption, authentication, and authorization.	Physical, cyber, complexity, interdependencies	
4.4	Efficient, Adaptable Encryption (B, A)	Makes intervention by adversary much more difficult.	New encryption technologies	G: Reduce chance of system compromise. C: Ensure no significant delays and no signal degradation.	Physical, cyber, complexity, interdependencies	
4.5	Robust Authentication and Authorization (B, A, ATD)	Reduce critical vulnerabilities.	Controls to SCADA and information networks	G: Develop standardized, efficient, easily deployed systems. C: Develop and implement controls.	Physical, cyber, complexity, interdependencies	
4.6	Intrusion Detection (B, A, ATD)	Critical for system protection and response.	Improved detection techniques	G: Ensure efficient algorithm with limited number of false alarms. C: Resolve issues of size and complexity of the system and short timeframe.	Physical, cyber, complexity, interdependencies	
4.7	Directed Energy Weapons Countermeasures (B, A)	Need better understanding of prevention, mitigation, and response.	Improved understanding of threat and responses	G: Understand threat and implement preventive measures. C: Prepare costs to design, build, and test such weapons.	Physical, cyber, complexity, interdependencies	

Table B.4 (Cont.)

R&D Topic No.	Title (Type[a])	Rationale	Product	Goals and Challenges	Threats and Vulnerabilities	Priority Category
5	Emergency Response and Recovery Information Technologies (B, A)	Mitigate urgent threat or vulnerability; cyber threats in electric grid are not well understood; potentially large consequences from not addressing this threat.	Protocols, policies, laws, computer simulation models, exercises, lessons learned	G: Detect attacks. C: Detect, discriminate, and develop technology; deregulate utilities.	Physical, cyber, interdependencies	Very important
6	Transmission and Distribution Technologies				Physical, cyber, complexity, interdependencies	Very important
6.1	Advanced Power Electronic Systems (ATD)	Reduced likelihood of cascading outages.	Hardware: improved FACTS, UPFC, SMES systems	G: Reduce costs and improve reliability. C: Develop hierarchical control systems.	Physical, cyber, complexity, interdependencies	
6.2	Instrumentation and Control (ATD, POP)	Improve operation and information; provide more options at crisis times; improve system reliability.	Hardware and software: improved two-way communications for load monitoring and control	G: Reduce costs and improve reliability. C: Proof of principle of reliability of large, "smart" systems.	Physical, cyber, complexity, interdependencies	
6.3	Upgrade Transmission System (ATD)	Improve margins to reduce likelihood of outages.	Hardware: increased capacity of above-ground transmission corridors	G: Enhance transmission capability. C: Conduct siting and determine environmental impact of new transmission capacity.	Physical, cyber, complexity, interdependencies	
6.4	Upgrade Distribution System (ATD)	Improve margins to reduce likelihood of local outages.	Hardware and software: technologies for reliable, smart, multidirectional distribution; application of solid-state power electronics to distribution	G: Enhance distribution capability. C: Develop large-scale simulation to assure reliability of complex system, harden system against sabotage and physical threats.	Physical, cyber, complexity, interdependencies	
6.5	Superconducting Transmission and Distribution (ATD, POP)	Improve efficiency and have a more secure system operation.	Hardware: demonstrations of distribution systems that use several km of HTSC cable	G: Enhance delivery capability C: Develop manufacturing techniques for long cables and thermal insulation with long-term reliability. Reduce cost. Complexity of system may make it vulnerable to sabotage.	Physical, cyber, complexity, interdependencies	

Table B.4 (Cont.)

R&D Topic No.	Title (Type[a])	Rationale	Product	Goals and Challenges	Threats and Vulnerabilities	Priority Category
7	On-line Security Assessment					Important
7.1	Incremental Algorithms (ATD)	Enable rapid calculations needed for on-line assessment.	Software: tools for perturbed problems (power flow, optimal power flow, eigen problems, coupled algebraic/ordinary differential equation problems)	G: Attain low-cost, fast-running problem solvers without sacrificing accuracy. C: Recognize and deal with complexity. Complete research in a short time.	Physical, cyber, complexity, interdependencies	
7.2	Geographic Decomposition Techniques (B, A, ATD)	Extend theoretical and numerical algorithms; improve performance for real-time control.	Software: tools for geographic decomposition in nonsymmetric complex cases	G: Increase speed of analysis to permit real-time control. C: Extend complex techniques to address real and reactive power components.	Physical, cyber, complexity, interdependencies	
7.3	Database Replication Techniques (B, A)	Specify large numbers of slightly different types of problems.	Software: methods for maintaining and replicating databases; advances in simulation query languages	G: Increase the size of databases and the ease of updating in real-time analyses. C: Resolve complex computational questions.	Physical, cyber, complexity, interdependencies	
8	Dispersed Generation and Backup Infrastructures					Important
8.1	Distributed Generation Systems (ATD, POP)	System more likely to withstand large-scale grid disturbances.	Hardware: demonstrations of distributed generation systems integrated with storage and controlled with custom power systems	G: Improve system reliability. C: Implement large-scale integration and simulation. Integrate massive amounts of advanced information and communications systems.	Physical, cyber, complexity, interdependencies	
8.2	Small-scale Power Generation Systems (ATD, POP)	Have a diverse supply; improve reliability.	Hardware: microturbines, fuel cells, and photovoltaic systems	G: Reduce costs and improve reliability, including the ability of systems to run unattended for long periods. C: Determine economics. Implement systems.	Physical, cyber, complexity, interdependencies	

Table B.4 (Cont.)

R&D Topic						
No.	Title (Type[a])	Rationale	Product	Goals and Challenges	Threats and Vulnerabilities	Priority Category
8.3	Advanced Backup Power Systems (ATD, POP)	System reliability needs to be improved to reduce the likelihood of large outages.	Hardware and software: integration of backup power systems into distributed generation networks to improve security	G: Improve system reliability. C: Apply control systems to existing backup generators, change policy to allow backup systems to power the distribution system in case of emergencies.	Physical, cyber, complexity, interdependencies	
9	Critical Consequence Analysis (B, A)	Modeling is needed for simulating complex systems.	Computerized model, model output identifying critical components	G: Identify critical components C: Collect data and determine model size.	Physical, complexity, interdependencies	Most important
10	Decision Support Systems (B, A, ATD, POP)	Decision analysis is effective in determining where best to allocate funds to mitigate risk.	Assessment reports, tool development	G: Identify risks and where money should be best spent to mitigate risk. C: Develop products to mitigate risk.	Physical, cyber, complexity, interdependencies	Most important
11	Physical Protection Assessment (B, A)	No comprehensive study has been completed in this area to date.	Report that will identify physical protection measures	G: Characterize current protection methods and determine advanced protecti on methods. C: Gain industry support.	Physical	Most important
12	Multisensor and Warning Technologies (B, A, ATD, POP)	Sensor and warning technologies can help mitigate vulnerabilities.	Technology reports, methodologies, product development	G: Implement industry-wide adoption of sensor and warning systems. C: Develop cost-effective standardized systems; ensure industry adopts technology.	Physical, cyber, complexity, interdependencies	Very important
13	Emergency Response Capability Enhancement (A)	No formal emergency channels currently exist.	Best-practices report, policy changes, work groups	G: Develop a formal national emergency plan and identify roles. C: Develop a partnership between industry and government.	Physical, cyber, complexity, interdependencies	Important
14	Cyber Protection Enhancement (B, A, ATD, POP)	No automated standards for system controls and electronic commerce systems. Systems lack standardized protocols and security measures.	Technology reviews, hardware and software development	G: Secure electronic commerce and SCADA capabilities. C: Develop cost-effective standar-dized systems, ensure adoption of technology by industry.	Physical, cyber, complexity, interdependencies	Most important

Table B.4 (Cont.)

R&D Topic						
No.	Title (Type[a])	Rationale	Product	Goals and Challenges	Threats and Vulnerabilities	Priority Category
15	Evaluation of Policy Effects (B, A)	Assure best interests of society, reduce system vulnerabilities	Appropriate policies for security	G: Understand connections between policy and system vulnerability impacts. C: Develop policies that use economic forces to improve security.	Complexity, interdependencies	Very important
16	Institutional Barriers (A)	Very broad infrastructure security cuts across government and industry; establish priorities and roles.	Development of partnerships, assessment of security tools, development of best practices	G: Prepare national infrastructure plan that addresses concerns, priorities, and roles. C: Cooperate, develop partnerships, and establish roles.	Physical, cyber, complexity, interdependencies	Most important
17	Infrastructure Interdependencies (B, A, ATD)	Determine how critical infrastructures depend upon each other for proper operation; develop mitigation strategies.	Reports analyzing current/future interdependencies/mitigation strategies; analysis tools	G: Improve understanding. C: Identify vulnerabilities and technical impacts, quantify/rank vulnerabilities and impacts, develop advanced modeling and simulation tools, identify mitigation strategies.	Physical, cyber, complexity, interdependencies	Most important

[a] B = basic; A = applied; ATD = advanced technology development; and POP = proof of principle and validation.

Table B.5 provides estimates of the timeframes and funding requirements by research topic. The total estimated funding required over the 1999–2015 period is $2.4 billion.

Table B.5 Summary of Funding Requirements by Research Topic

R&D Research Topic		Timeframe (yr)	Funding Requirement[a]
No.	**Description**		
1	Real-time control mechanisms		
1.1	Instrumentation and monitoring for distributed control	3–15	130
1.2	Analysis and computing for large-scale systems	3–10	100
1.3	Advanced control methods	3–10	88
1.4	Decision support tools	5–15	85
	Sum of 1.1–1.4	3–15	**Subtotal, 403**
2	Analysis of scale and complexity	3–5	75
3	Vulnerability assessment	1–12	35
4	Information assurance and cyber security		
4.1	Threat assessment and risk management	3–5	25
4.2	Large systems analysis	5–10	45
4.3	High-security SCADA systems	5–10	80
4.4	Efficient, adaptable encryption	3–10	75
4.5	Robust authentication and authorization	3–10	75
4.6	Intrusion detection	3–10	75
4.7	Directed energy weapons countermeasures	3–10	60
	Sum of 4.1–4.7	3–10	**Subtotal, 435**
5	Emergency response and recovery information technologies	3–12	10
6	Transmission and distribution technologies	1–15	>500
7	On-line security assessment	1–15	50
8	Dispersed generation and backup infrastructures	1–15	100
9	Critical consequence analysis	1–4	3
10	Decision support systems	10	120
11	Physical protection assessment	1–3	5
12	Multisensor and warning technologies	1–10	160
13	Emergency response capability enhancement	1–5	152
14	Cyber protection enhancement	1–12	201
15	Evaluation of policy effects	1–5	35
16	Institutional barriers	1–6	74
17	Infrastructure interdependencies	1–15	31

[a] Funding requirements are estimated cumulative amounts in millions of U.S. dollars over the timeframe shown. Some topics, such as transmission and distribution technologies, will have substantial contributions from industry. At a minimum, a modest federal role, emphasizing infrastructure assurance considerations, is needed.

Section 4
R&D Topic Roadmaps

This section outlines the R&D topic roadmaps, which describe the research pathway, including the timeframe and sequence of activities required to achieve the specified goals. The roadmap is communicated most simply in a table (Table B.6) that identifies the elements of the R&D topics over time. The R&D topics are listed in the same order as they appeared in Section 3.

Table B.6 Summary of the Energy R&D Roadmap

R&D Topic No.	R&D Topic Title	Achieved by ~2000	Achieved by ~2005	Achieved by ~2010
1	Real-time Control Mechanisms			
1.1	Instrumentation and Monitoring for Distributed Control	Implement common data model and identify measurement requirements.	Develop advanced sensors, measurement timing standards, and data compression tools. Establish high bandwidth communication channels.	Establish wide area monitoring, data storage and retrieval, and adaptive monitoring methods.
1.2	Analysis and Computing for Large-scale Systems	Implement on-line security assessment tools.	Establish stability indices. Develop measurement-based analysis tools and parameters for integrating measurement- and model-based tools.	Establish uncertainty theory and implement integrated analytical approach.
1.3	Advanced Control Methods	Assess current state of robust control theory and decentralized control theory.	Advance theoretical basis for robust and decentralized control.	Develop proof of principle and validation on integrated large-scale system control theory.
1.4	Decision Support Tools	Develop new visualization techniques and operator interfaces for increased data volume.	Implement first-generation reasoning tools. Develop tools to assist operators in handling many transactions.	Develop autonomous agents and implement multiconstraint optimization tools.
2	Analysis of Scale and Complexity	Study restructuring effects on complexity. Develop theoretical understanding of complex systems and applied understanding of the evolving complexity of the power grid.	Develop an understanding of human interfaces and how humans handle scale and complexity. Understand effects of uncertainties on vulnerability and develop mitigation methods.	
3	Vulnerability Assessment	Complete systematic and current estimates of vulnerabilities and threats. Estimate impacts of outages. Define modeling requirements. Characterize restructuring effects.	Develop or enhance models. Analyze restructuring impacts. Evaluate infrastructure assurance options.	Develop improved procedures and evaluate more options.
4	Information Assurance and Cyber Security			
4.1	Threat Assessment and Risk Management	Conduct systematic, industry-wide threat assessment and vulnerability mapping. Develop base risk management tools.	Develop standardized, industry-wide threat model. Integrate risk management tools into design tools. Ensure consistent models are used to define threat environments and assess risk. Integrate models into design and validation tools.	

Table B.6 (Cont.)

R&D Topic No.	Title	Achieved by ~2000	Achieved by ~2005	Achieved by ~2010
4.2	Large Systems Analysis	Develop basic models and simulations and basic design tools.	Develop integrated models and near real-time prediction, model-based control.	Validate the entire power grid. Incorporate models into design. Develop simulation and validation tools.
4.3	High-security SCADA Systems	Develop a baseline understanding of existing systems and current industry practices. Develop design guidelines.	Develop and validate proof of concept. Standardize efforts for deployment of new SCADA networks.	Produce and adopt standard SCADA design guidelines.
4.4	Efficient, Adaptable Encryption	Develop a baseline understanding of requirements for major system areas. Evaluate encryption technologies.	Deploy encryption technologies throughout the power industry.	Deploy dynamic and high-bandwidth encryption.
4.5	Robust Authentication and Authorization	Map the requirements for authentication and authorization of existing systems. Define general-purpose, scalable mechanisms. Begin working with standards.	Work with the electric power industry and product manufacturers to adopt standardized mechanisms.	Implement standardized authentication and authorization models on all new systems added to the grid.
4.6	Intrusion Detection	Develop understanding of threats and current vulnerabilities. Deploy threat detection to both the communication and control infrastructure of the grid.	Develop and deploy efficient, dynamic intrusion detection tools.	Link intrusion detection into central threat center for grid-wide system monitoring. Deploy automated response capability.
4.7	Directed Energy Weapons Countermeasures	Develop understanding of the current state of high-energy weapons. Construct and test devices. Develop test bed. Prepare design guidelines for protection.	Integrate information learned into overall design tools.	Conduct further research into directed energy weapons.
5	Emergency Response and Recovery Information Technologies	Develop concept. Identify critical components and protection and mitigation strategies. Begin developing exercise process and computer simulation models.	Conduct exercises on a periodic basis. Develop and apply lessons learned from exercises. Begin developing concept for oil and natural gas pipeline networks.	Refine process as changes warrant. Begin conducting exercises for oil and gas pipeline networks.
6	Transmission and Distribution Technologies	Examine specific infrastructure assurance contributions for several R&D topics. Improve siting and environmental impact process for new transmission lines.	Develop hardware and software. Complete proof of principle for smart instrumentation and control systems. Make progress in advanced power electronics systems.	Achieve significant progress in superconducting technologies. Implement advanced power electronics systems.

Table B.6 (Cont.)

R&D Topic No.	Title	Achieved by ~2000	Achieved by ~2005	Achieved by ~2010
7	On-line Security Assessment	Examine incremental algorithms for system perturbations. Obtain 1,000-fold increase in speed with subcycle state information. Develop database replication techniques.	Reduce cost and running times. Develop accurate tools and models for the national grid. Develop tools for geographic decomposition in nonsymmetric complex cases.	Develop and implement improved and new tools. Reduce cost and running times.
8	Dispersed Generation and Backup Infrastructures	Analyze infrastructure assurance benefits of dispersed generation. Prioritize options.	Demonstrate and integrate distributed generation systems with storage. Demonstrate and control with custom power systems. Develop improved backup system.	Continue reducing costs and improving reliability of technology options. Improve ability for systems to run unattended for long periods.
9	Critical Consequence Analysis	Complete and implement basic design of model.	Develop incident/failure scenarios and consequence analysis, including curtailment impacts, by using the model.	
10	Decision Support Systems	Assess data and tools. Assign decision analysis requirements with priorities.	Develop expert system tools. Make models for highest priority items. Assess secondary priority items.	Continue to develop high-priority items. Develop expert system tools and models for secondary priority items.
11	Physical Protection Assessment	Collect historic reports and data. Survey industry to determine highest vulnerabilities. Assess technology. Develop and implement strategies.		
12	Multisensor and Warning Technologies	Assess current technologies. Design needed technologies. Establish industry-government partnership.	Roadmap national technologies. Develop software and hardware.	Implement technology pilot program. Commercially develop technologies. Set up an oversight committee.
13	Emergency Response Capability Enhancement	Develop industry-government partnership. Establish roles for government and industry. Identify technology gaps.	Develop roles. Develop a national emergency plan. Begin technology implementations.	Ensure that technologies and best practices are widely implemented in industry.
14	Cyber Protection Enhancement	Identify encryption algorithms and standards.	Complete technology review and selection. Manufacture chips.	Implement **e**nhanced protection system for SCADA and electronic commerce. Obtain acceptance of approved standards by industry.
15	Evaluation of Policy Effects	Determine the effect of numerous proposed policies on vulnerability and security of energy systems. Explore grid operation implications.	Establish college programs that deal with technical and public policy aspects of infrastructure assurance.	
16	Institutional Barriers	Develop partnerships.	Develop tools and roles and establish	Maintain support and networking

Table B.6 (Cont.)

R&D Topic No.	Title	Achieved by ~2000	Achieved by ~2005	Achieved by ~2010
			priorities.	needs, such as the FBI security center.
17	Infrastructure Interdependencies	Relate technical complexities to business disruptions and economic losses. Complete in-depth analysis of technical impacts. Examine requirements for advanced computational modeling and simulation tools.	Identify and analyze options to reduce interdependency impacts. Develop analysis tools.	Obtain results of analyzing options to reduce interdependency-related vulnerabilities.